AMERICAN
JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

VOLUME LXXVII

1955

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXXVII, Number 1
JANUARY, 1955

THE JOHNS HOPKINS PRESS
BALTIMORE 18, MARYLAND
U. S. A.

CONTENTS

The AMERICAN JOURNAL OF MATHEMATICS appears four times yearly.

The subscription price of the JOURNAL is $8.50 in the U. S.; $8.75 in Canada; and $9.00 in other foreign countries. The price of single numbers is $2.50.

Manuscripts intended for publication in the JOURNAL should be sent to Professor AUREL WINTNER, The Johns Hopkins University, Baltimore 18, Md.

Subscriptions to the JOURNAL and all business communications should be sent to THE JOHNS HOPKINS PRESS, BALTIMORE 18, MARYLAND, U. S. A.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

GENERALIZED GALOIS THEORY FOR RINGS WITH MINIMUM CONDITION, II.*

By Tadasi Nakayama.

In our first paper, "Generalized Galois theory for rings with minimum condition, *Amer. J. Math.*, vol. 73 (1951), pp. 1-12—referred to as I—we gave a certain Galois theory for primary rings with minimum condition. The theory contains the Cartan-Jacobson [1], [2] Galois theory for sfields, at least as far as the main Galois correspondence is concerned. But the "inner" portion of the Galois group, there considered, comes from a certain completely primary subring. Now that we are dealing with a general primary ring, satisfying the minimum condition, it is desirable to consider a wider class of Galois groups whose inner portions come from general primary subrings rather than from completely primary ones. In fact in another paper [5] we have developed a Galois theory for simple rings, with minimum condition, in which the Galois groups have rather satisfactory generality and have inner portions consisting of inner automorphisms effected by regular elements of simple subalgebras. Combining the methods and results of this paper with those in I, we now give a Galois theory for primary rings which deals with Galois groups of the generality required above, though it fails to cover the theory of I completely. Our main Galois correspondence is given in **2**, Theorem 1, our "regular" Galois group being defined both at the opening of **2** and in succession to Theorem 1.

Moreover, after a study of a certain special type of factor-groups of the Galois group (**3**, Theorem 2), we prove an extension theorem for isomorphisms (**3**, Theorem 3), to recover a second main aspect of Galois theory which was neglected in our first paper I.

(*Corrections*: The condition i) in I, Theorem 2 was stated incorrectly. There we were to assume further that K has an independent Z-basis such that the corresponding left-multiplications on R constitute an independent R_r-basis of R_rK_l. On the other hand, the condition iv) there was stated in a rather awkward form. We had to assume only that every inner automorphism of R effected by a regular element of K belongs to Φ. (For the fact that this, supported by the other conditions, implies iv), cf. **1** below.)

* Received June 30, 1954.

Further, I, Lemma 4 should, as G. Azumaya has kindly pointed out, refer only to a primary ring R; the primarity is needed to secure the existence of a system of elements $a_1, a_2, \cdots, a_s$ in K, asserted on page 7, line 17 there, such that $\gamma_1, \cdots, \gamma_t, a_{1l}, \cdots, a_{sl} \bmod N_rK_l$ together form an independent R_r/N_r-right-basis of R_rK_l/N_rK_l. But, since we considered only primitive rings in Theorem 2 there, the validity of our main result of the paper I remains unaffected.

The same lemma was used also in an older paper [3]. The writer wishes to take this opportunity to make the correction that the final theorem (3. 2) in that paper should refer only either to a primary ring R or to the case where K modulo the radical N of R contains the center of the residue-ring R/N; it is easy to see that also in the last case the existence of $a_1, \cdots, a_s$ as above is secured.)

1. Preliminaries. We first cite some of our previous results which we need in the sequel. Let R be a ring satisfying the minimum condition (for left- and right-ideals) and possessing a unit element 1. With a subset X of R we denote by X_l, X_r the sets of the left and the right multiplications in R by the elements of X. Let $\mathfrak{A}$ be the absolute endomorphism ring of R as a module. If $\mathfrak{F}$ is any subset of $\mathfrak{A}$, the commuter subring $V_{\mathfrak{A}}(\mathfrak{F})$ of $\mathfrak{F}$ in $\mathfrak{A}$ is nothing but the $\mathfrak{F}$-endomorphism ring of R. In particular, if Φ $(\subseteq \mathfrak{A})$ is a group of automorphisms of R and if S is the invariant system of Φ in R, then $S_r = V_{\mathfrak{A}}(R_l\Phi)$. First, we consider an automorphism group Φ of R satisfying the following conditions:

i$_0$) Φ is complete in the sense that the subgroup Φ_0 of Φ consisting of the inner automorphisms of R contained in Φ is the set of all inner automorphisms effected by the regular elements of a certain subring K of R containing the center Z of R,

i$_1$) K is generated by its regular elements,

i$_2$) K has a (linearly) independent finite basis $a_1 = 1, a_2, \cdots, a_k$ over Z such that $a_{1r}, a_{2r}, \cdots, a_{kr}$ are independent over R_l,

i$_3$) R is a regular module of R_lK_r, or, which amounts to the same, the direct sum R^k of k copies of R is R_lK_r-right-isomorphic with R_lK_r itself (For the notions of regular modules and their ranks cf. I, footnote 7),

ii) The factor group $G = \Phi/\Phi_0$ is finite, and if $\{\rho(1) = 1, \rho(\sigma), \cdots, \rho(\tau)\}$ is a representative system of Φ modulo Φ_0 $(G = \{1, \sigma, \cdots, \tau\})$, the R_l-two-sided modules R_l, $\rho(\sigma)R_l$ $(\sigma \neq 1)$ have no isomorphic composition residue-modules (If this holds for any one representative system then the same is the case for any other representative system).

If Φ satisfies these conditions, then R is regular also with respect to the operator ring $R_l\Phi$ and we have not only $S_r = V_{\mathfrak{A}}(R_l\Phi)$ but also

$$V_{\mathfrak{A}}(S_r) = R_l\Phi = \sum_{\sigma} \rho(\sigma) R_l K_r, \tag{1}$$

where S is the invariant system of Φ in R. Moreover, R possesses an independent right-basis of $(G:1)k$ terms over S (I, Theorem 1; everything is stated here in the left-right symmetric form to I). The number $(G:1)k = (\Phi:\Phi_0)k$ is called the *reduced order* of Φ.

LEMMA 0. *Let R be primary and let its subring K satisfy the condition i_2). Let $\mathfrak{M}$ be an R_l-two-sided submodule of R_lK_r such that $\mathfrak{M}N_l = \mathfrak{M} \cap N_lK_r$, where N is the radical of R, and $\mathfrak{M}/\mathfrak{M}N_l$ is R_l/N_l-right-regular (These last two conditions are certainly satisfied when $\mathfrak{M}$ is R_l-right-regular, because of the primarity of R). Then $\mathfrak{M}$ is a direct summand of the R_l-two-sided module R_lK_r and has also an independent finite basis over R_l consisting of elements of K_r.*

Our old proof, in I, Lemma 4, remains valid, since the existence of $a_1, a_2, \cdots, a_s$ as asserted there is now true; cf. the correction in the introduction.

Let R be primary and let ϕ be an automorphism of R leaving the invariant system S of Φ elementwise fixed, Φ being as above. Then $\phi \in V_{\mathfrak{A}}(S_r) = \sum_{\sigma} \rho(\sigma) R_l K_r$ and $\phi R_l = R_l \phi$. So ϕR_l $(= R_l\phi)$ is an R_l-two-sided submodule of $\sum \rho(\sigma) R_l K_r$, and is, as such, a direct sum of submodules of $\rho(\sigma) R_l K_r$, σ running over G; observe the condition ii). As R (whence R_l) is primary (and is thus two-sided directly indecomposable), we see that there exists a σ such that (cf. I, Lemma 2)

$$\phi \in \rho(\sigma) R_l K_r. \tag{2}$$

Putting $\phi_0 = \rho(\sigma)^{-1}\phi$, we have $\phi_0 \in R_l K_r$. Also ϕ_0 is an automorphism of R, leaving S elementwise fixed, and thus $\phi_0 R_l = R_l \phi_0$. It follows from Lemma 0 that $\phi_0 R_l$ $(= R_l \phi_0)$ has the form $R_l a_r$ $(a \in K)$. Putting $\phi_0 = b_l a_r$ $(b \in R)$ and observing $1^{\phi_0} = 1$ we see that (a is regular and) $b = a^{-1}$. Thus ϕ_0 is an inner automorphism of R effected by a regular element of K. So $\phi_0 \in \Phi_0$ and $\phi = \rho(\sigma)\phi_0 \in \Phi$; this point was left rather obscure in I. Hence, *Φ exhausts the automorphisms of R leaving S elementwise fixed (provided that R is primary).*

Another use we want to make of Lemma 0 is, as in I, to study the structure of the endomorphism ring of R with respect to the right multiplica-

tion of a certain subring of R. Let T be a subring of R which contains the invariant system S of our automorphism group Φ (satisfying the above conditions). Then the T_r-endomorphism ring of R is a subring of $V_{\mathfrak{A}}(S_r) = \sum \rho(\sigma) R_l K_r$ and contains R_l. By virtue of ii) we have

$$V_{\mathfrak{A}}(T_r) = \sum \rho(\sigma) U_\sigma \tag{3}$$

with certain R_l-two-sided submodules U_σ of $R_l K_r$. Suppose that R is T_r-regular. Then $V_{\mathfrak{A}}(T_r)$ is R_l-right-regular. Hence each U_σ is a direct sum of submodules R_l-right-isomorphic to directly indecomposable right-ideal direct components of R_l. R being assumed to be primary, this means that each U_σ is R_l-right-regular. So our lemma may be applied to yield

LEMMA 1. *Let R be primary and T_r-regular, T being a subring of R containing S. Then each U_σ in* (3) *has the form $U_\sigma = R_l L_r^{(\sigma)}$, where $L^{(\sigma)}$ is a subring of K containing Z and possessing an independent finite basis over Z such that the corresponding right multiplications on R constitute an independent basis of U_σ over R_l. We have, therefore,*

$$V_{\mathfrak{A}}(T_r) = \sum_\sigma \rho(\sigma) R_l L_r^{(\sigma)}. \tag{4}$$

Now, the case of a simple ring R was studied in our paper [5]. We need the following main result there:

Let R be a simple ring, satisfying minimum condition and possessing unit element 1, and let Φ be an automorphism group of R which is regular in the sense that it satisfies i_0) with a simple subring K finite over the center Z of R and Φ/Φ_0 is finite; then i_1), i_2), i_3) and ii) are all automatically fulfilled. The invariant system S of Φ in R is a simple subring of R whose commuter $V_R(S)$ in R is K. The regular subgroups of Φ are in 1-1 Galois correspondence with the simple subrings of R containing S and possessing simple commuters in R, and any isomorphism between two such simple subrings of R leaving S elementwise fixed is induced by an element of Φ ([5], Theorems 5, 6).

2. Galois theory for primary rings. Let R be a primary ring, with minimum condition and unit element 1. Let N be its radical, and Z its center. We call a group of automorphisms of R *regular* when it satisfies the conditions i_0), i_2) and ii) in **1** and when, moreover, the subring K is such that $((K+N)/N$ is simple and) the product in R/N of $(K+N)/N$ and the center of R/N is simple. It is clear that this definition is in accord with the notion of a regular automorphism group for the case of a simple ring R, as defined in [5] (cf. the end of the preceding section).

For any subset A of $\mathfrak{A}$ leaving N set-wise invariant we denote by A^0 the set of endomorphisms of the residue-module R/N induced by the elements of A; we identify equal endomorphisms of R/N induced by distinct elements of A. So, in particular, $R_l{}^0$ and $R_r{}^0$ are the left- and right-multiplication rings of the residue ring R/N.

Now we observe that a regular automorphism group, as just defined, satisfies also the conditions i_1) and i_3) (whence what we have stated for a group satisfying i_0), i_1), i_2), i_3) and ii) can certainly be applied to it). It is clear that i_1) is fulfilled. In order to verify i_3), we prove first

LEMMA 2. *Let K be a subring of our primary ring R which satisfies the condition i_2); thus let $(a_1 = 1, a_l, \cdots, a_k)$ be an independent Z-basis of K such that $(a_{1r}, a_{2r}, \cdots, a_{kr})$ is an independent R_l-basis of R_lK_r. Then the endomorphisms of R/N induced by $a_{1r}, a_{2r}, \cdots, a_{kr}$ (i. e. $a_{1r}{}^0, a_{2r}{}^0, \cdots, a_{kr}{}^0$) are independent over the left-multiplication ring $R_l{}^0$ of R/N. In particular, $a_1 \bmod N, a_2 \bmod N, \cdots, a_k \bmod N$ are independent over the center of R/N, and the intersection of $(K+N)/N$ and the center of R/N is exactly $(Z+N)/N$. If we have i_3), besides i_2), then R/N is an $R_l{}^0K_r{}^0$-regular module.*

Proof. Suppose

$$\sum_{i=1}^{k} s_{il}{}^0 a_{ir}{}^0 = 0$$

for some elements s_i in R. We have $\sum_i s_i x a_i \,\varepsilon\, N$ for all x in R. Hence $l(N)\sum_i s_i x a_i = 0$ for all x in R, where $l(N)$ denotes the left annihilator of N in R. Since $a_{1r}, a_{2r}, \cdots, a_{kr}$ are independent over R_l, we have $l(N)s_i = 0$, for every $i = 1, 2, \cdots, k$. So each s_i is contained in the right annihilator $r(l(N))$ of $l(N)$. But $r(l(N)) = N$; this is in fact the only point where the primarity is used in our proof. Thus $s_i \,\varepsilon\, N$ $(i = 1, 2, \cdots, k)$, which proves the first assertion of our lemma. The second one follows easily from the first.

Now suppose that i_3) holds. Then the R_lK_r-right-module R_lK_r is isomorphic to R^k, the direct sum of k copies of R, and the R_lK_r-right-module $R_lK_r/N_lK_r = R_lK_r/(R_lK_r)N_l$ is isomorphic to $(R/RN_l)^k = (R/N)^k$. Here

$$\begin{aligned} R_lK_r/N_lK_r &\cong (R_l/N_l)a_{1r} \oplus (R_l/N_l)a_{2r} \oplus \cdots \oplus (R_l/N_l)a_{kr} \\ &\cong R_l{}^0 a_{1r}{}^0 \oplus R_l{}^0 a_{2r}{}^0 \oplus \cdots \oplus R_l{}^0 a_{kr}{}^0 \end{aligned}$$

by the first half of our lemma. It follows that the $R_l{}^0K_r{}^0$-right-module $R_l{}^0K_r{}^0$ is isomorphic to $(R/N)^k$.

Next,

LEMMA 3. *Let a subring K of the primary ring R satisfy* i_2) *and suppose that the product* $((K+N)/N)$ (*center of* R/N) *is simple. Then R is R_lK_r-regular, i.e.* i_3) *is satisfied.*

Proof. Since R/N is centrally simple over its center, the product $R_l{}^0K_r{}^0$ (which is (homomorphic, whence) isomorphic to the direct (Kronecker) product $(R/N) \otimes ((K+N)/N)$ (center of R/N)) over the center of R/N) is a simple ring. Thus its right-module R/N is $R_l{}^0K_r{}^0$-regular and $(R/N)^k$ is $R_l{}^0K_r{}^0$-isomorphic to $R_l{}^0K_r{}^0$, where k is the Z-rank of K (which is, according to Lemma 2, equal to the $R_l{}^0$-rank of $R_l{}^0K_r{}^0$). Now let u be an element of R^k such that $u \bmod N^k$ corresponds to the unit element of $R_l{}^0K_r{}^0$ by our $R_l{}^0K_r{}^0$-isomorphism of $(R/N)^k = R^k/N^k$ and $R_l{}^0K_r{}^0$. We consider the submodule $u(R_lK_r)$ of R^k. On mapping the unit element of R_lK_r onto u, we obtain an R_lK_r-homomorphism of R_lK_r onto $u(R_lK_r)$. If we pass to the residue-module $R^k/N^k = (R/N)^k$ the image $u(R_lK_r) \bmod N^k$ is all of R^k/N^k, since the mapping clearly induces our $R_l{}^0K_r{}^0$-isomorphism between $R_l{}^0K_r{}^0$ and R^k/N^k. However, as N^k is the intersection of all maximal R_l-submodules of R^k, it follows that $u(R_lK_r) = R^k$, too. Considering R_l-lengths, we conclude that our homomorphism mapping (which has thus been shown to be onto R^k) is an isomorphism between R_lK_r and R^k. This proves our lemma.

Remark. As our proof shows, our second assumption, in Lemma 3, may be replaced by the assumption that R/N be $R_l{}^0K_r{}^0$-regular.

We have thus seen that a regular automorphism group of R satisfies all the conditions in **1**.

Another remark we want to make is that if Φ is a regular automorphism group of our R then the automorphism group Φ^0 of the simple residue-ring R/N, induced by Φ, is a regular automorphism group of R/N, with the product $((K+N)/N)$ (center of R/N) as the associated simple subring of R/N generated by the elements of R/N effecting inner automorphisms of R/N contained in Φ^0. In fact, in order to see this we have only to observe that for $\sigma \neq 1$ the (minimal) R_l-two-sided modules R_l/N_l, $\rho(\sigma)R_l/\rho(\sigma)N_l$ are not isomorphic, or, which is the same, the $R_l{}^0$-two-sided modules $R_l{}^0$, $\rho(\sigma)^0R_l{}^0$ are not isomorphic, which is in turn equivalent to saying that $\rho(\sigma)^0$ is not an inner automorphism of the simple ring R/N, a consequence of ii).

It follows, either from I, Theorem 1 or from [5] that R/N possesses an independent right-basis of $(G:1)k$ terms over the invariant system, in R/N, of Φ^0. On the other hand, R has an invariant right-basis of $(G:1)k$ terms over the invariant system S, in R, of Φ. Here $(S+N)/N$ is clearly contained in the invariant system of Φ^0. It follows then that the invariant

system of Φ^0 is exactly $(S+N)/N$. Hence $(S+N)/N$ is a simple ring. It follows further that an independent S-right-basis of R is independent over $(S+N)/N$ when considered modulo N. Thus we have

LEMMA 4. *Let Φ be a regular automorphism group of a primary ring R, possessing unit element and satisfying minimum condition, and let S be the invariant system of Φ in R. Then $(S+N)/N$, with N the radical of R, is the invariant system of the automorphism group Φ^0 of R/N induced by Φ. So $(S+N)/N$ is simple. (An independent S-right-basis of R exists and) an independent S-right-basis of R forms, when considered modulo N, an independent $(S+N)/N$-right-basis of R/N.*

Let S be the invariant system of a regular automorphism group Φ of our primary ring R. Consider a subring T of R which contains S;

$$R \supseteq T \supseteq S. \tag{5}$$

Suppose that $T+N/N$ is simple. As $(T+N)/N \supseteq (S+N)/N$ and $(S+N)/N$ is the invariant system of Φ^0 (as has been shown above) $(T+N)/N$ is a weakly normal simple subring of R/N, and hence R/N is $R_l{}^0T_r{}^0$ fully reducible; see [5], § 1. So, if we denote by $R^{(0)}$ the intersection of all maximal R_lT_r-submodules of R, then

$$N \supseteq R^{(0)}, \quad \text{whence} \quad l(N)R^{(0)} = 0. \tag{6}$$

Now we assert that none of $R^{\rho(\sigma)a_r}$ $(a \in K, a \notin N)$, σ running over G (cf. **1**, ii)), is contained in $R^{(0)}$. For, suppose $R^{\rho(\sigma)a_r} \subseteq R^{(0)}$. Then, with the left annihilator $l(N)$ of N, we have $l(N)R^{\rho(\sigma)a_r} = 0$, or $\rho(\sigma)a_rl(N)_l = 0$, $a_rl(N)_l = 0$, $l(N)Ra = 0$, whence $Ra \subseteq N$ and $a \in N$ contrary to the assumption. Naturally this applies to the case when a is any one of the basic elements $a_1, a_2, \cdots, a_k$ of K over Z.

Suppose further that R has an independent basis over our intermediate ring T. Then the T_r-endomorphism ring $V_{\mathfrak{A}}(T_r)$ of R has the form (4), $V_{\mathfrak{A}}(T_r) = \sum \rho(\sigma)R_lL_r{}^{(\sigma)}$, where each $R_lL_r{}^{(\sigma)}$ has an independent R_l-basis consisting of elements of $L_r{}^{(\sigma)}$ (Lemma 1). In particular, $L_r{}^{(1)}$ $(\rho(1)=1)$ is $V_{\mathfrak{A}}(T) \cap R_r$ which is the R_lT_r-endomorphism ring of R;

$$L^{(1)} = V_R(T). \tag{7}$$

Put $L = L^{(1)}$ for the sake of simplicity. Then $L_r\rho(\sigma)R_lL_r{}^{(\sigma)}L_r \subseteq V_{\mathfrak{A}}(T_r)$ whence $\subseteq \rho(\sigma)R_lL_r{}^{(\sigma)}$,, and it follows that each $L^{(\sigma)}$ is L-two-sided allowable.

Now, decompose R into a direct sum of directly indecomposable R_lT_r-right-submodules $\mathfrak{m}_i$; $R = \mathfrak{m}_1 \oplus \mathfrak{m}_2 \oplus \cdots \oplus \mathfrak{m}_s$. Suppose that the $\mathfrak{m}_i$ are

all mutually R_lT_r-isomorphic, or, which is the same, that $L = V_R(T)$ is primary; observe that $L_r = V_{\mathfrak{A}}(R_lT_r)$. On fixing a coherent system of isomorphisms among the $\mathfrak{m}_i$, we denote by $\{\epsilon_{ij}\}$ the corresponding system of matric units in the R_lT_r-endomorphism ring L_r of R. Let a be an element of K such that $a \not\in N$. Then, as was shown above,

$$R^{\rho(\sigma)a_r} \not\subseteq R^{(0)}, \tag{8}$$

where $R^{(0)}$ is the intersection of all maximal R_lT_r-submodules of R. Hence the image by $\rho(\sigma)a_r$ of one, at least, of $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_s$ is not contained in $R^{(0)}$, and we may assume, without loss in generality, that

$$\mathfrak{m}_1{}^{\rho(\sigma)a_r} \not\subseteq R^{(0)}. \tag{9}$$

Then there exists an i such that the projection $\mathfrak{m}_1{}^{\rho(\sigma)a_r\epsilon_{ii}}$ of $\mathfrak{m}_1{}^{\rho(\sigma)a_r}$ on $\mathfrak{m}_i$ is not contained in $R^{(0)}$. We have, with such an i,

$$\mathfrak{m}_1{}^{\rho(\sigma)a_r\epsilon_{ii}\epsilon_{i1}} \not\subseteq R^{(0)}. \tag{10}$$

Consider now a σ with $L^{(\sigma)} \neq 0$. Then $L^{(\sigma)} \not\subseteq N$; in fact $R_lL_r{}^{(\sigma)}$ has an independent basis over R_l consisting of elements of $L_r{}^{(\sigma)}$ (which is not void). So we may take an element a in $L^{(\sigma)}$ not contained in N, and apply our consideration to this a so as to obtain (10), with this a. There $\rho(\sigma)a_r\epsilon_{ii}\epsilon_{i1} = \rho(\sigma)a_r\epsilon_{i1}$ is an $(R_l, \rho(\sigma))$-semilinear and T_r-linear endomorphism of R; observe that $a_r, \epsilon_{i1} \in V_{\mathfrak{A}}(R_l)$ and $\rho(\sigma)a_r, \epsilon_{i1} \in V_{\mathfrak{A}}(T_r)$. It induces an endomorphism on $\mathfrak{m}_1$, which is not nilpotent. For, if it were, then the image would be contained in any maximal R_lT_r-submodule of R, whence in $R^{(0)}$, contrary to (10). By Fitting's lemma (in a generalized formulation as in Jacobson's book, Theory of Rings, Math. Surveys II, New York 1943, for example) $\rho(\sigma)a_r\epsilon_{i1}$ induces therefore an $((R_l, \rho(\sigma))$-semilinear and T_r-linear) automorphism on $\mathfrak{m}_1$ (Let $R_l \cup T_r$ be the operator domain Ω in Jacobson's book).

As $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_s$ are by assumption all $\{R_l, T_r\}$-isomorphic, it follows then that $R = \sum \mathfrak{m}_i$ has an $(R_l, \rho(\sigma))$-semilinear and T_r-linear automorphism, say α. Since $\alpha \in V_{\mathfrak{A}}(T_r)$ and αR_l ($\subseteq \mathfrak{A}$) is R_l-two-sided isomorphic with $\rho(\sigma)R_l$, we have

$$\alpha R_l \subseteq V_{\mathfrak{A}}(T_r) \cap \rho(\sigma)R_lK_r = \rho(\sigma)R_lL_r{}^{(\sigma)}.$$

So $\alpha R_lL_r \subseteq \rho(\sigma)R_lL_r{}^{(\sigma)}$. On the other hand, every element of $\alpha^{-1}\rho(\sigma)R_lL_r{}^{(\sigma)}$ is $\{R_l, T_r\}$-linear and it follows that $\alpha^{-1}\rho(\sigma)R_lL_r{}^{(\sigma)} \subseteq \rho(1)R_lL_r = R_lL_r$. Combining these two relations we have

$$\rho(\sigma)R_lL_r{}^{(\sigma)} = \alpha R_lL_r. \tag{11}$$

Moreover, as $\alpha^{-1}\rho(\sigma)$ is contained in both R_lL_r and $V_{\mathfrak{A}}(R_l) = R_r$, we have $\alpha^{-1}\rho(\sigma) \varepsilon R_lL_r \cap R_r = L_r$ and $\alpha^{-1}\rho(\sigma) = b_r$ with an element b in L. Here b is regular (since $\alpha^{-1}\rho(\sigma)$ is a (module-) automorphism) and $b_l^{-1}\alpha^{-1}\rho(\sigma) = b_l^{-1}b_r$ is the inner ring-automorphism of R effected by b. Hence $b_l^{-1}\alpha^{-1}$ is a ring-automorphism of R. It is T_r-linear, i. e. it is a ring-automorphism of R leaving T elementwise fixed. Putting $\rho^*(\sigma) = \alpha b_l$, we have $\rho^*(\sigma) = \rho(\sigma)b_r^{-1}b_l \varepsilon \rho(\sigma)\Phi_0$ and $\rho^*(\sigma)$ is an element of Φ which is a representative of the coset $\rho(\sigma)\Phi_0$ of $\rho(\sigma)$ modulo Φ_0. Moreover $\rho(\sigma)R_lL_r^{(\sigma)} = \alpha R_lL_r = \rho^*(\sigma)b_l^{-1}R_lL_r = \rho^*(\sigma)R_lL_r$. Now, these hold for each σ with $L^{(\sigma)} \neq 0$. It is clear, from these considerations, that the totality of such σ form a subgroup, say, H, of G. So we have proved

LEMMA 5. *Let T be a subring of R containing the invariant system S of a regular automorphism-group Φ in R. Suppose that $(T+N)/N$ is simple, that R possesses an independent right-basis over T, and that the commuter $L = V_R(T)$ of T in R is primary. Then there exist a representative system $\{\rho^*(1) = 1, \rho^*(\sigma), \cdots, \rho^*(\tau)\}$ of Φ modulo Φ_0 and a subgroup H of G such that*

$$V_{\mathfrak{A}}(T_r) = \sum_{\sigma \varepsilon H} \rho^*(\sigma)R_lL_r. \tag{12}$$

L has an independent finite basis over Z such that the corresponding right multiplications on R constitute an independent R_l-basis of R_lL_r.

It is also clear that the subgroup Ψ of all elements of Φ leaving our T element-wise fixed is

$$\Psi = \bigcup_{\sigma \varepsilon H} \rho^*(\sigma)\Psi_0 \tag{13}$$

where Ψ_0 is the totality of inner automorphisms of R effected by regular elements of L, and

$$V_{\mathfrak{A}}(T_r) = R_l\Psi. \tag{14}$$

Further, $T_r = V_{\mathfrak{A}}(R_l\Psi)$ and T is the invariant system of Ψ. Thus

LEMMA 6. *Let T be as in Lemma 5, and let Ψ be the totality of automorphisms of R (or, of elements of Φ) leaving T element-wise fixed. Then T is the invariant system of Ψ in R.*

Now, Ψ clearly satisfies the conditions i_0), i_2) and ii), with K replaced by L (and Φ, Φ_0 by Ψ, Ψ_0, naturally). So Ψ is a regular automorphism-group if we assume that the product of $(L+N)/N$ and the center of R/N is simple. We observe also that this last condition implies that $((L+N)/N$ is simple and) L is primary. Thus

LEMMA 7. *Let T be a subring of R containing the invariant system S*

of a regular automorphism group Φ in R. Suppose that $(T+N)/N$ is simple, that R has an independent right-basis over T, and that the product $((L+N)/N)$ (center of R/N) in R/N is simple, where $L=V_R(T)$. Then the totality Ψ of automorphisms of R (or, elements of Φ) leaving T element-wise fixed is a regular automorphism group of R.

Next we start, conversely, with a regular subgroup Ψ of Φ, and let T be its invariant system. To Ψ and T we may naturally apply what we know about Φ and S. Thus Ψ exhausts the automorphisms of R leaving T element-wise fixed and (T is primary and) $(T+N)/N$ is simple. Combining this with Lemmas 5 and 6, we have our main

THEOREM 1. *Let R be a primary ring possessing a unit element and satisfying the minimum condition. Let Φ be a regular group of automorphisms of R and let S be the invariant system of Φ in R. Then (S is primary and) $(S+N)/N$ is simple, where N denotes the radical of R. R possesses an independent right-basis over S, the number of elements in the basis being equal to the reduced order of Φ, and Φ exhausts the automorphisms of R leaving S element-wise fixed. Further, the regular subgroups of R are in a 1-1 Galois correspondence with the intermediate rings T of R and S such that R possesses an independent right basis over T, $(T+N)/N$ is simple and, if $L=V_R(T)$ is the commuter of T in R, (L is primary and) the product $((L+N)/N)$ (center of R/N) is simple.*

For the sake of convenience, we repeat our definition of a regular automorphism group: a group Φ of automorphisms of R is called *regular* if the following conditions i), ii) are satisfied:

i) the totality Φ_0 of inner automorphisms of R contained in Φ is the totality of inner automorphisms of R effected by the regular elements in a certain subring K containing the center Z of R, generated by its regular elements, and possessing an independent finite basis $a_1, a_2, \cdots, a_k$ over Z (we may take $a_1=1$) such that $a_{1r}, a_{2r}, \cdots, a_{kr}$ are independent over R_l, and the product $((K+N)/N)$ (center of R/N) is simple, N being the radical of R,

ii) the factor group $G=\Phi/\Phi_0$ is finite, and, if $\{\rho(1), \rho(\sigma), \cdots, \rho(\tau)\}$ $(G=1, \sigma, \cdots, \tau)$ (we may take $\rho(1)=1$) is a representative system of Φ modulo Φ_0, the R_l-two-sided modules R_l, $\rho(\sigma)R_l$ $(\sigma\neq 1)$ have no isomorphic composition residue-modules.

The number $(G:1)(K:Z)$ is called the *reduced order* of the regular automorphism group Φ.

We note that our regular automorphism groups cross with the automorphism-groups considered in I in their generality, though the present groups are perhaps better qualified to be called Galois groups for primary rings.

3. Certain factor-groups of a regular automorphism group; extension of isomorphisms. Let Φ be an automorphism group of a ring R, with unit element and minimum condition, which satisfies the conditions i_0), i_1), i.), i_3), and ii). Consider a subgroup Ψ of Φ which satisfies similar conditions, L with $R_l\Psi \cap R_r = L_r$ replacing K and $\Psi_0 = \Phi_0 \cap \Psi$ replacing Φ_0. Let T be the invariant system in R of Ψ. R possesses over T an independent right basis of $(\Psi:\Psi_0)(L:Z)$ terms, and Ψ is the totality of automorphisms of R leaving T element-wise fixed. $V_{\mathfrak{A}}(T_r)$ has the form

$$R_l\Psi_0\rho^*(1) \oplus R_l\Psi_0\rho^*(\alpha) \oplus \cdots \oplus R_l\Psi_0\rho^*(\gamma),$$

where $\{\rho^*(1), \rho^*(\alpha), \cdots, \rho^*(\gamma)\}$ is a representative system, in Ψ, of the group $H = \{1, \alpha, \cdots, \gamma\} = \Psi/\Psi_0$ (which may be considered as a subgroup of $G = \Phi/\Phi_0$.

Assume now that Ψ is an invariant subgroup of Φ. Then T is mapped on itself by every element of Φ, and the factor-group Φ/Ψ is an automorphism group of T. We first prove

LEMMA 8. *Let ϕ be an element of Φ. If the T_l-two-sided modules T_l and ϕT_l have some isomorphic composition residue-modules, then $\phi \in \Phi_0\Psi$.*

Proof. For any T-double-module $\mathfrak{m}$ we can construct an R-T-double-module $R \otimes_T \mathfrak{m}$. Further, if ϕ is an automorphism of T, we may construct from $\mathfrak{m}$ a T-double-module $(\phi, \mathfrak{m})$ by crossing the operation of T on the left-hand side of $\mathfrak{m}$ with ϕ; thus $(\phi, \mathfrak{m})$ is identical with $\mathfrak{m}$ as T-right-module, while the left-operation of an element a of T on $(\phi, \mathfrak{m})$ coincides with that of a^ϕ on $\mathfrak{m}$. Now, if ϕ is induced by an automorphism of R, denoted again by ϕ, then we assert that the similarly defined R-T-double-module $(\phi, R \otimes_T \mathfrak{m})$ is (R-T-) isomorphic with $R \otimes_T (\phi, \mathfrak{m})$. In fact, this can easily be verified by taking an independent T-right-basis $(x_1, x_2, \cdots, x_h)$ of R and using the independent bases $(x_i^{\phi^{-1}})$ and (x_i) respectively in constructing $R \otimes_T (\phi, \mathfrak{m})$ and $(\phi, R \otimes_T \mathfrak{m})$; cf. [4], § 5.

We consider the case where $\mathfrak{m}$ is T itself and ϕ is an element of Φ. Naturally we have then $R \otimes_T \mathfrak{m} = R \otimes_T T = R$. Put $f = (\Psi:\Psi_0)(L:Z)$. Then R has an independent right-basis of f terms over T, and the direct sum R^f of f copies of R is $V_{\mathfrak{A}}(T_r)$-isomorphic with $V_{\mathfrak{A}}(T_r)$. The $V_{\mathfrak{A}}(T_r)$-endomorphism ring of R^f is the f-dimensional matric ring $(T_r)_f$ over T_r,

while that of $V_{\mathfrak{A}}(T_r)$ is of course the left-multiplication ring of $V_{\mathfrak{A}}(T_r)$ which we shall denote by $\mathfrak{T}$. Hence there exists a (ring-) isomorphism λ between $(T_r)_f$ and $\mathfrak{T}$ which corresponds to a $V_{\mathfrak{A}}(T_r)$-isomorphism between R^f and $V_{\mathfrak{A}}(T_r)$. Thus R^f and $V_{\mathfrak{A}}(T_r)$ are $V_{\mathfrak{A}}(T_r)$-(linear) and $((T_r)_f — \mathfrak{T}, \lambda)$-semilinear isomorphic. They are in particular R_l-linear and $((T_r)_f — \mathfrak{T}, \lambda)$-semilinear isomorphic, for $R_l \subseteq V_{\mathfrak{A}}(T_r)$. We construct from R^f a second $\{R_l, (T_r)_f\}$-module $(R^f)^{(\phi)}$ by crossing the operator domain R_l with its automorphism ϕ. Similarly we construct $V_{\mathfrak{A}}(T_r)^{(\phi)}$. These two bodies are also R_l-(linear) and $((T_r)_f — \mathfrak{T}, \lambda)$-semilinear isomorphic.

Suppose now that the $\{R_l, T_r\}$-modules R and $R^{(\phi)}$ have some (properly linear) isomorphic composition residue-modules. Then the same is the case with the $\{R_l, (T_r)_f\}$-modules R^f and $R^{(\phi)f} = (R^f)^{(\phi)}$. In view of the above R_l-linear and $\{(T_r)_f — \mathfrak{T}, \lambda\}$-semilinear isomorphisms between R^f, $V_{\mathfrak{A}}(T_r)$ and between $(R^f)^{(\phi)}$, $V_{\mathfrak{A}}(T_r)^{(\phi)}$, we see that the $\{R_l, \mathfrak{T}\}$-modules $V_{\mathfrak{A}}(T_r)$ and $V_{\mathfrak{A}}(T_r)^{(\phi)}$ have some (properly linear) isomorphic composition residue-modules. This means however that the $V_{\mathfrak{A}}(T_r)$-R_l-double-modules $V_{\mathfrak{A}}(T_r)$, $V_{\mathfrak{A}}(T_r)\phi$ $(\subseteq \mathfrak{A})$ have some isomorphic composition residue-modules. Naturally the same is the case if we consider $V_{\mathfrak{A}}(T_r)$, $V_{\mathfrak{A}}(T_r)\phi$ merely as R_l-double-modules. But $V_{\mathfrak{A}}(T_r) = R_l\Psi = \sum_{\alpha \varepsilon H} R_l\Psi_0\rho^*(\alpha)$. Hence there are α, β in H such that $R_l\Psi_0\rho^*(\alpha)$, $R_l\Psi_0\rho^*(\beta)\phi$ have isomorphic composition residue-modules. It follows that $\Psi_0\rho^*(\alpha) \equiv \Psi_0\rho^*(\beta)\phi \bmod \Phi_0$ whence $\phi \,\varepsilon\, \Phi_0\Psi$.

Now, the assumption in our lemma, that the T_l-double-modules T_l, ϕT_l have some isomorphic composition residue-modules, is equivalent to assuming that the T-double-modules T and (ϕ, T) have some isomorphic composition residue-modules. This implies, because of our remark at the beginning of the present proof, that the R-T-double-modules R and (ϕ, R) have some isomorphic composition residue-modules. This is in turn equivalent to the existence of isomorphic composition residue-modules of the $\{R_l, T_r\}$-modules R and $R^{(\phi)}$, from which we have derived $\phi \,\varepsilon\, \Phi_0\Psi$. So our lemma is proved.

We have now immediately

THEOREM 2. *Let R be a ring, with unit element and minimum condition, and let Φ be an automorphism group of R satisfying the conditions* i$_0$), i$_1$), i$_2$), i$_3$) *and* ii), *with its subgroup Φ_0 as in* i$_0$). (*It is sufficient that R be primary and Φ a regular automorphism group of R*). *Let Ψ be an invariant subgroup of Φ which contains Φ_0 and let T be the invariant system of Ψ in R. Then Φ/Ψ is a regular automorphism-group of T containing no inner automorphism of T except the unity.*

(Automorphism groups of the type of this factor-group have been studied

in [4], § 5 and the older paper in Jour. Math. Soc. Japan 1 (1949), pp. 203-216 cited there.)

Next we prove an extension theorem for isomorphisms of subrings (Theorem 3). To do so, we again consider an automorphism group Φ of a primary ring R, with unit element and minimum condition, which fulfills the conditions i_0), i_1), i_2), i_3) and ii) of **1**. Let S be its invariant system. We have $V_{\mathfrak{A}}(S_r) = R_l\Phi = \sum_{\sigma \varepsilon G} \rho(\sigma) R_l\Phi_0$, $R_l\Phi_0 = R_lK_r$. Let T be a subring of R which contains S and over which R has an independent right-basis. By Lemma 1, $V_{\mathfrak{A}}(T_r)$ has the form (3), i.e. $V_{\mathfrak{A}}(T_r) = \sum_{\sigma} \rho(\sigma) R_lL_r^{(\sigma)}$; each subring $L^{(\sigma)}$ of K contains Z and possesses an independent basis over Z such that the corresponding right-multiplications on R constitute an independent basis of $R_lL_r^{(\sigma)}$ over R_l.

Now, let α be a (ring-) isomorphic mapping of T into R which leaves S element-wise fixed. We assume that R has also an independent right-basis over T^α. Let $\{x_i\}$, $\{y_i\}$ be independent right-bases of R over T, T^α respectively; they consist of equal numbers of elements, since the T_r- and the T_r^α-ranks of R are equal as we readily see on considering S_r-ranks. The mapping

$$\sum x_it_i \to \sum y_it_i^\alpha \qquad (t_i \varepsilon T) \tag{15}$$

gives a $(T_r - T_r^\alpha, \alpha)$-semilinear automorphism μ of R. Let $\mathfrak{M}$ be the totality of $(T_r - T_r^\alpha, \alpha)$-semilinear endomorphisms of R; clearly $\mu \varepsilon \mathfrak{M}$. $\mathfrak{M}$ is an R_l-two-sided submodule of $V_{\mathfrak{A}}(S_r)$. So $\mathfrak{M}$ is a direct sum of submodules of $\rho(\sigma)R_lK_r$ $(\sigma \varepsilon G)$;

$$\mathfrak{M} = \sum_{\sigma} (\rho(\sigma)R_lK_r \cap \mathfrak{M}).$$

Further, $\mathfrak{M}\mu^{-1} \subseteq V_{\mathfrak{A}}(T_r)$ and $V_{\mathfrak{A}}(T_r)\mu \subseteq \mathfrak{M}$, whence

$$\mathfrak{M} = V_{\mathfrak{A}}(T_r)\mu = \sum \rho(\sigma)R_lL_r^{(\sigma)}\mu. \tag{16}$$

It follows that $\mathfrak{M}$ is R_l-left-regular. Its direct summands $\mathfrak{M} \cap \rho(\sigma)R_lK_r$ are then also R_l-left-regular. Lemma 0 implies that for each σ

$$\rho(\sigma)^{-1}\mathfrak{M} \cap R_lK_r = R_lM_r^{(\sigma)}, \tag{17}$$

where $M^{(\sigma)}$ is, for each σ, a certain submodule of K (Apply Lemma 0 in its modified form with right-operations replaced by left-operations (but retaining R_l, K_r), or in its completely (right-left) symmetric form with R replaced by a ring inverse-isomorphic to R). Hence

$$\mathfrak{M} \cap \rho(\sigma)R_lK_r = \rho(\sigma)R_lM_r^{(\sigma)}.$$

Denote now by $\bar{R}^{(0)}$ the intersection of all the maximal $R_lT_r^\alpha$-submodules

of R. As $\mathfrak{M}$ contains a (module-) automorphism μ, we have $R\mathfrak{M} = R$ and $R\mathfrak{M} \not\subseteq \bar{R}^{(0)}$. There exists, therefore, a $\tau \varepsilon G$ such that

$$(R\rho(\tau)R_l M_r^{(\sigma)} =)\ R(\mathfrak{M} \cap \rho(\tau)R_l K_r) \not\subseteq \bar{R}^{(0)}.$$

Fixing such a τ, we take an element m in $M^{(\sigma)}$ such

$$R\rho(\tau)m_r \not\subseteq \bar{R}^{(0)}. \tag{18}$$

Let

$$R = \mathfrak{m}_1 \oplus \mathfrak{m}_2 \oplus \cdot\cdot\cdot \oplus \mathfrak{m}_s \tag{19}$$

be a direct decomposition of R into directly indecomposable $R_l T_r$-submodules. There exists an index i such that $\mathfrak{m}_i \rho(\tau) m_r \not\subseteq \bar{R}^{(0)}$. We may, without loss of generality, assume

$$\mathfrak{m}_1 \rho(\tau) m_r \not\subseteq \bar{R}^{(0)}. \tag{20}$$

Further, let

$$R = \bar{\mathfrak{m}}_1 \oplus \bar{\mathfrak{m}}_2 \oplus \cdot\cdot\cdot \oplus \bar{\mathfrak{m}}_{\bar{s}} \tag{21}$$

be a direct decomposition of R into directly indecomposable $R_l T_r^{\alpha}$-submodules. There exists an index j such that the $\bar{\mathfrak{m}}_j$-projection, with respect to (21), of $\mathfrak{m}_1 \rho(\tau) m_r$ is not contained in $\bar{R}^{(0)}$.

Next, let $\bar{\mathfrak{M}}$ be the totality of $(T_r^{\alpha} - T_r, \alpha^{-1})$-semilinear endomorphisms of R, and let $R^{(0)}$ be the intersection of all the maximal $R_l T_r$-submodules of R. Clearly $\mu^{-1} \varepsilon \bar{\mathfrak{M}}$, $\bar{\mathfrak{M}} = \sum(\bar{\mathfrak{M}} \cap \rho(\sigma)R_l K_r)$ and each $\bar{\mathfrak{M}} \cap \rho(\sigma)R_l K_r$ has the form $\rho(\sigma)R_l \bar{M}_r^{(\sigma)}$ with a subring $\bar{M}^{(\sigma)}$ of K. Let u be an element of $\bar{\mathfrak{m}}_j$ which is not contained in $\bar{R}^{(0)}$; observe that $\bar{\mathfrak{m}}_j \cap \bar{R}^{(0)}$ is the intersection of all the maximal $R_l T_r^{\alpha}$-submodules of $\bar{\mathfrak{m}}_j$. Then we assert that

$$u\mu^{-1} \not\varepsilon R^{(0)}. \tag{22}$$

To see this, we observe that μ, being an element of $\sum \rho(\sigma)R_l M_r^{(\sigma)}$, is a sum of elements of the form $\rho(\sigma)a_l m_r^{(\sigma)}$ ($a \varepsilon R$, $m^{(\sigma)} \varepsilon M^{(\sigma)}$). Since R is primary, we may choose the a's so that they are regular elements of R. Such a product $\rho(\sigma)a_l m_r^{(\sigma)}$, with a regular in R, is an R_l-semilinear endomorphism of R; the associated automorphism of R is the product of $\rho(\sigma)$ and the inner automorphism of R effected by a. As it is in $\mathfrak{M}$, it is also $(T_r - T_r^{\alpha}, \alpha)$-semilinear. Hence it maps $R^{(0)}$ into $\bar{R}^{(0)}$. For, if we denote by U the counter-image of $\bar{R}^{(0)}$ by $\rho(\sigma)a_l m_r^{(\sigma)}$, then R/U is mapped R_l-semilinear and $(T_r - T_r^{\alpha}, \alpha)$-semilinear isomorphically upon a certain $R_l T_r^{\alpha}$-submodule of $R/\bar{R}^{(0)}$. As $R/R^{(0)}$ is $R_l T_r^{\alpha}$-fully-reducible, it follows that R/U is $R_l T_r$-fully-reducible. Hence $U \supseteq R^{(\sigma)}$, or, which is the same, $\rho(\sigma)a_l m_r^{(\sigma)}$ maps $R^{(0)}$ into

$\bar{R}^{(0)}$. Therefore, μ itself maps $R^{(0)}$ into $\bar{R}^{(0)}$. Now, if we had $u\mu^{-1} \varepsilon R^{(0)}$, then $u = u\mu^{-1}\mu \varepsilon R^{(0)}\mu \subseteq \bar{R}$, which is a contradiction. So we have (22).

We have seen that there exists an index j such that the $\bar{\mathfrak{m}}_j$-projection of $\mathfrak{m}_1\rho(\tau)m_r$ is not contained in $\bar{R}^{(0)}$. Taking as our u (which has been assumed only to be an element of $\bar{\mathfrak{m}}_j$ not belonging to $\bar{R}^{(0)}$) an element in the $\bar{\mathfrak{m}}_j$-projection of $\mathfrak{m}_1\rho(\tau)m_r$ not contained in $\bar{R}^{(0)}$, we see that

$$(\bar{\mathfrak{m}}_j\text{-projection of } \mathfrak{m}_1\rho(\tau)m_r)\mu^{-1} \not\subseteq R^{(0)}.$$

As $\mu^{-1} \varepsilon \mathfrak{M} = \sum(\mathfrak{M} \cap \rho(\sigma)R_lK_r)$, there exist an element $\bar{\tau}$ in G and an element $\bar{m}$ in $\bar{M}^{(\bar{\tau})}$ such that

$$(23) \qquad (\bar{\mathfrak{m}}_j\text{-projection of } \mathfrak{m}_1\rho(\tau)m_r)\rho(\bar{\tau})\bar{m}_r \not\subseteq R^{(0)}.$$

There exists then an index i such that the $\mathfrak{m}_i$-projection of the left-hand side of (23) is not contained in $R^{(0)}$.

Now, we assume that $\mathfrak{m}_1, \mathfrak{m}_2, \cdots, \mathfrak{m}_s$ are all R_lT_r-(linear) isomorphic and $\bar{\mathfrak{m}}_1, \bar{\mathfrak{m}}_2, \cdots, \bar{\mathfrak{m}}_{\bar{s}}$ are all $R_lT_r^{\alpha}$-isomorphic, or what is the same, both $V_R(T_r) = L^{(1)}$ and $V_R(T_r^{\alpha}) = \bar{L}^{(1)}$ are primary. Let $\{\epsilon_{hk}\}$, $\{\bar{\epsilon}_{pq}\}$ be the systems of matric unit R_lT_r- and $R_lT_r^{\alpha}$-endomorphisms of R with respect to (19) and (21), respectively. Naturally $\epsilon_{hk} \varepsilon L_r^{(1)}$ $(= (V_R(T))_r = V_{\mathfrak{A}}(R_lT_r))$ and $\epsilon_{pq} \varepsilon \bar{L}^{(1)}$. Our above result shows that, with suitable i, j, τ, $\bar{\tau}$, m $(\varepsilon M^{(\tau)})$ and $\bar{m}$ $(\varepsilon M^{(\bar{\tau})})$,

$$\mathfrak{m}_1\rho(\tau)m_r\bar{\epsilon}_{jj}\rho(\bar{\tau})\bar{m}_r\epsilon_{ii} \not\subseteq R^{(0)} \text{ whence } \not\subseteq \mathfrak{m}_i \cap R^{(0)}, \text{ and, therefore,}$$

$$(24) \qquad m_1\rho(\tau)m_r\bar{\epsilon}_{jj}\rho(\bar{\tau})\bar{m}_r\epsilon_{i1} \not\subseteq \mathfrak{m}_1 \cap R^{(0)}.$$

Here $\rho(\tau)m_r\bar{\epsilon}_{jj}\rho(\bar{\tau})\bar{m}_r\epsilon_{i1}$ is $(R_l, \rho(\tau)\rho(\bar{\tau}))$-semilinear. It is, on the other hand, T_r-linear, for $\rho(\sigma)m_r$ $(\varepsilon \mathfrak{M})$ is $(T_r - T_r^{\alpha}, \alpha)$-semilinear and $\rho(\bar{\tau})\bar{m}_r$ $(\varepsilon \bar{\mathfrak{M}})$ is $(T_r^{\alpha} - T_r, \alpha^{-1})$-semilinear while $\bar{\epsilon}_{jj}$ and ϵ_{i1} are respectively T_r^{α}- and T_r linear. As in **2**, we apply Fitting's lemma, in its generalized formulation, to the directly indecomposable R_lT_r-module $\mathfrak{m}_1$. It asserts that $\rho(\tau)m_r\bar{\epsilon}_{jj}\rho(\bar{\tau})\bar{m}_r\epsilon_{i1}$ induces on $\mathfrak{m}_1$ either an ($(R_l, \rho(\tau)\rho(\bar{\tau}))$-semilinear and T_r-linear) automorphism or a nilpotent endomorphism. If the latter were the case, then $\mathfrak{m}_1$ would be mapped, by $\rho(\tau)m_r\bar{\epsilon}_{jj}\rho(\bar{\tau})\bar{m}_r\epsilon_{i1}$, into each maximal R_lT_r-submodule of $\mathfrak{m}_1$, whence into $\mathfrak{m}_1 \cap R^{(0)}$, contrary to (24). Hence $\rho(\tau)m_r\bar{\epsilon}_{jj}\rho(\bar{\tau})\bar{m}_r\epsilon_{i1}$ induces an automorphism on $\mathfrak{m}_1$.

It follows that $\rho(\tau)m_r\bar{\epsilon}_{jj}$ maps $\mathfrak{m}_1$ isomorphically into $\bar{\mathfrak{m}}_j$. As $\rho(\tau)m_r\bar{\epsilon}_{jj}$ is $(T_r - T_r^{\alpha}, \alpha)$-semilinear, whence S_r-linear, we see that the S_r-rank of $\mathfrak{m}_1$ is at most equal to the S_r-rank of $\bar{\mathfrak{m}}_j$, which is naturally equal to that of $\bar{\mathfrak{m}}_1$. Interchanging the roles of T, T^{α} we see similarly that the S_r-rank of $\bar{\mathfrak{m}}_1$ is at most equal to that of $\mathfrak{m}_1$. Hence they are equal and $\rho(\tau)m_r\bar{\epsilon}_{jj}$ induces an

$(R_l, \rho(\tau))$-semilinear and $(T_r - T_r^{\alpha}, \alpha)$-semilinear isomorphism of $\mathfrak{m}_1$ onto $\bar{\mathfrak{m}}_j$. As $\bar{\mathfrak{m}}_j$ is $R_l T_r^{\alpha}$-isomorphic to $\bar{\mathfrak{m}}_1$, we have thus established the existence of an $(R_l, \rho(\tau))$-semilinear and $(T_r - T_r^{\alpha}, \alpha)$-semilinear isomorphism between $\mathfrak{m}_1$ and $\bar{\mathfrak{m}}_1$ (or between any $\mathfrak{m}_k$ and any $\bar{\mathfrak{m}}_p$). We now find readily that the numbers s, $\bar{s}$ in (19), (21) are equal. For each $k = 1, 2, \cdots, s$ there exists an $(R_l, \rho(\tau))$-semilinear and $(T_r - T_r^{\alpha}, \alpha)$-semilinear isomorphism between $\mathfrak{m}_k$, $\bar{\mathfrak{m}}_k$ and there exists therefore a (module-) automorphism of R of the same kind, say ϕ. As $\phi^{-1}R_l\phi = R_l$ and $R_r = V_{\mathfrak{A}}(R_l)$ we have $\phi^{-1}R_r\phi = R_r$ and the inner automorphism of $\mathfrak{A}$ effected by its regular element ϕ induces a (ring)-automorphism of R_r. It induces on T_r the isomorphism α with T^{α}. This shows that the isomorphism α between T and T^{α} is extended to a (ring-) automorphism of R. The extended automorphism belongs to Φ, since it leaves S element-wise fixed. So we have

THEOREM 3. *Let Φ be an automorphism group of a primary ring R, with unit element and minimum condition, which satisfies the conditions* i_0), i_1), i_2), i_3) *and* ii) (*of* 1), *and let S be its invariant system* (It is sufficient that Φ be a regular automorphism group of R). *Let T be a subring of R containing S and having a primary commuter $V_R(T)$ in R, and let α be an isomorphic mapping of T into R leaving S element-wise fixed such that the commuter $V_R(T^{\alpha})$ of the image T^{α} is also primary. Then α can be extended to an element of Φ.*

NAGOYA UNIVERSITY.

REFERENCES,

[1] H. Cartan, "Théorie de Galois pour les corps non-commutatifs," *Annales Scientifiques de l'École Normale Superiere*, vol. 65 (1948), pp. 60-77.

[2] N. Jacobson, "A note on division rings," *American Journal of Mathematics*, vol. 69 (1947), pp. 27-36.

[3] T. Nakayama, "Commuter systems in a ring with radical," *Duke Mathematical Journal*, vol. 16 (1947), pp. 331-337.

[4] ———, "Automorphisms of simple, complete primitive, and directly indecomposable rings," *Annals of Mathematics*, vol. 55 (1952), pp. 538-551.

[5] ———, "Galois theory of simple rings," *Transactions of the American Mathematical Society*, vol. 73 (195–), pp. 276-292.

PERIODIC MAPPINGS ON BANACH ALGEBRAS.*

By Bertram Yood.

1. Introduction. Let B be a real Banach algebra. In investigations of such algebras, those with an involution (adjoint operation) have received special attention. By an involution is meant an anti-automorphism of period two. Here we study automorphisms and anti-automorphisms T of B periodic with finite period (the period of T is the smallest positive integer n such that $T^n = I$, where I is the identity).

The norms $\| x \|$ and $\| x \|_1 = \| T(x) \|$ are two Banach algebra norms for B which are equivalent if and only if T is continuous ([1], p. 41). The equivalence of two Banach algebra norms for B has been discussed by Rickart [10] where it is shown that a necessary and sufficient condition for the equivalence is that $S = (0)$ where S is the separating ideal of the two norms, the set of elements x where for some sequence $\{x_n\}$ in B, $\| x_n - x \| \to 0$ and $\| x_n \|_1 \to 0$. As shown in [10], S is a closed two-sided ideal of B consisting entirely of topological divisors of zero. A further property of S is (Theorem 2.4) that either the two norms are equivalent or S is a radical algebra in the sense of the Brown-McCoy radical [2]. Our approach to the question of the continuity of T is made through the study of the corresponding ideal S.

It has been conjectured [10] that any two Banach algebra norms for a semi-simple algebra B are equivalent. This would imply the continuity of any periodic T defined on B. In this direction we show, in Theorem 4.6, that if every automorphism and anti-automorphism T of period two defined on each closed semi-simple sub-algebra B_1 of B is continuous then any T of period 2^n defined on B is continuous. Furthermore if B is semi-simple, the period n of $T = 3$ or 2^m and if the set $\{x \in B \mid (I + T + \cdots + T^{n-1})(x) = 0\}$ is closed, then T is continuous.

2. Definitions and preliminaries. Let T be a linear mapping defined on an algebra B over the real field whose range is B and which has period n. Suppose that, for each x, y in B either $T(xy) = T(x)T(y)$ or $T(xy) = T(y)T(x)$. By a result of Hua [4] one of these two equations holds throughout B and T is either an automorphism or an anti-automorphism. Let

$$P_n = (I + T + \cdots + T^{n-1})/n$$

* Received April 26, 1954.

where I is the identity. Let

$$H = \{x \varepsilon B \mid T(x) = x\} \quad \text{and} \quad K = \{x \varepsilon B \mid P_n(x) = 0\}.$$

If $P_n(x) = x$ then $x = TP_n(x) = T(x)$, $x \varepsilon H$ and conversely $x \varepsilon H$ implies that $P_n(x) = x$. It is then clear that P_n is a projection of B on H and that H and K are complementary linear manifolds, $B = H \oplus K$.

2.1. LEMMA. *$T(H) = H$. $T(K) = K$. $T^i(x) - x \varepsilon K$ for all $x \varepsilon B$ and all positive integers i.*

The first statement is clear. If $x \varepsilon K$ then $TP_n(x) = P_nT(x) = 0$ and $T(K) \subset K$. By iteration we obtain $T^{-1}(K) = T^{n-1}(K) \subset K$. Thus $T(K) = K$. If $y = T^i(x) - x$ then a simple computation shows that $P_n(y) = 0$.

Now for each integer i, $i = 1, \cdots, n-1$, T^i is also periodic. We define H_i andK_i as the sets H and K above corresponding to the mappings T^i.

2.2. LEMMA. *Let T have period n. Then for $i = 1, 2, \cdots, n-1$ the following hold.*

(a) $H_1 \subset H_i$, $K_i \subset K_1$.

(b) $H_i = H_1 \oplus H_i \cap K_1$, $K_1 = K_i \oplus H_i \cap K_1$.

(c) $H_1 = H_i$ *if and only if* $K_1 = K_i$.

(d) *If i divides n then $H_i \cap K_1$ is the null-space of $I + T + \cdots + T^{i-1}$.*

(e) *If i divides n then $H_1 = H_i$ if and only if $I + T + \cdots + T^{i-1}$ is one-to-one.*

(a). Let $y \varepsilon K_i$, α be the greatest common divisor of i and n and set $c = n/\alpha$. By the definition of K_i we obtain

$$y + T^{\alpha}(y) + \cdots + T^{(c-1)\alpha}(y) = 0. \tag{1}$$

If we operate on (1) by $T, T^2, \cdots, T^{\alpha-1}$ and add we obtain $P_n(y) = 0$ or $y \varepsilon K_1$.

(b). It is clear that $H_i \supset H_1 \oplus H_i \cap K_1$. Let $x \varepsilon H_i$, $x = u + v, u \varepsilon H_1$, $v \varepsilon K_1$. Then $x = T^i(x) = u + T^i(v) = u + v$. Thus $v \varepsilon H_i \cap K_1$. For the second formula of (b) note that

$$B = H_i \oplus K_i = H_1 \oplus [K_i \oplus H_i \cap K_1] = H_1 \oplus K_1$$

where, by (a), $K_i \oplus H_i \cap K_1 \subset K_1$. Thus $K_1 = K_i \oplus H_i \cap K_1$.

(c). $H_i = H_1$ (or $K_i = K_1$) if and only if $H_i \cap K_1 = 0$.

(d). Let $n = ci$. Set $V = I + T + \cdots + T^{i-1}$ and $W = I + T^i + T^{2i} + \cdots + T^{(c-1)i}$. When $WV = VW = I + T + \cdots + T^{n-1}$. If $x \varepsilon H_i \cap K_1$ then $W(x) = cx$. $VW(x) = 0$ so that $V(x) = 0$. Conversely if $V(x) = 0$ then $WV(x) = 0$ so that $x \varepsilon K_1$. Also $(TV - V)(x) = 0$ where $TV - V = T^i - I$. Thus $x \varepsilon H_i$.

(e). This follows from (b) and (d).

2.3. Lemma. *Let $v \varepsilon K_1$, $y \varepsilon H_1$. Then $vy + yv \varepsilon K_1$.*

Note that $T^i(vy + yv) = T^i(v)y + yT^i(v)$. Thus $P_n(vy + yv) = 0$.

Let B be a real Banach algebra which is a Banach algebra under two norms $\| x \|$ and $\| x \|_1$. An element s in B is said ([10], p. 619) to *separate* the norms if there exists a sequence x_n in B such that $\| s - x_n \| \to 0$ and $\| x_n \|_1 \to 0$. The set S of all elements which separate the two norms has been shown by Rickart ([10], p. 621) to be a two-sided ideal in B, closed with respect to both norms and each of whose elements is a topological divisor of zero with respect to both norms. S will be called the *separating ideal* for these two norms. The same separating ideal is obtained if the roles of $\| x \|$ and $\| x \|_1$ are interchanged. The two norms are equivalent if and only if S is the zero element.

Consider next an automorphism or anti-automorphism U of period n. Define $\| x \|_1 = \| U(x) \|$. Following ideas of Rickart ([9], p. 1068) we show that $\| x \|_1$ is a Banach algebra norm for B.

It is clear that the norm makes B_1 into a normed linear space. Moreover $\| xy \|_1 = \| U(xy) \| \leqq \| U(x) \| \| U(y) \| = \| x \|_1 \| y \|_1$. Also if $\| x_m - x_n \|_1 \to 0$ as $m, n \to \infty$ then there exists $y \varepsilon B$ such that $\| y - U(x_n) \| \to 0$. Then $\| U^{-1}(y) - x_n \|_1 \to 0$ so that B is Banach algebra under the norm $\| x \|_1$. The separating ideal S for the two norms $\| x \|$ and $\| x \|_1$ is called the *separating ideal for U.*

If S is the separating ideal corresponding to two Banach algebra norms $\| x \|$ and $\| x \|_1$ for B then $\| x \|$ and $\| x \|_1$ are two Banach algebra norms on S and thus there is a separating ideal $S_1 \subset S$ corresponding to the two norms.

2.4. Theorem. *Let $\| x \|$ and $\| x \|_1$ be two Banach algebra norms for B with separating ideal S and with separating ideal S_1 with respect to S. Then S and S_1 have the following properties.*

(1) *$x_1x_2 \varepsilon S_1$ if $x_i \varepsilon S$, $i = 1, 2$. S_1 is a two-sided ideal of B.*

(2) *S_1 is contained in no proper regular (one-sided or two-sided) ideal of S.*

(3) *Either the two norms are equivalent on B or S is a radical algebra in the Brown-McCoy sense.*

(4) *If the two norms are equivalent on S, then S is a zero algebra.*

(1). *Let* $y_n \varepsilon B$, $\| y_n - x_1 \| \to 0$, $\| y_n \|_1 \to 0$. Then $\| y_n x_2 - x_1 x_2 \| \to 0$ and $\| y_n x_2 \|_1 \to 0$ where $y_n x_2$ and $x_1 x_2 \varepsilon S$. Thus $x_1 x_2 \varepsilon S_1$. The second statement is shown in a similar way.

(2). Let J be, say, a proper regular right ideal in S with e as a left identity of S modulo J. If $S_1 \subset J$ then, since $ex - x \varepsilon J$ for all $x \varepsilon S$ and $ex \varepsilon S_1$ by (1), we have $S \subset J$ which is impossible.

(3). Suppose that the two norms are not equivalent. Then $S \neq (0)$. From the results of Brown and McCoy ([2], p. 51) we see that S is a radical algebra in the sense of their radical if and only if S contains no maximal regular two-sided ideal. However if M is such an ideal in S, results of Rickart ([10], p. 621) show that $S_1 \subset M$. By (2) the latter is impossible.

(4). If the two norms are equivalent on S then $S_1 = (0)$ and (4) then follows from (1).

As applied to a commutative Banach algebra B, Theorem 2.4 shows that S is then a radical algebra contained in the radical of B. This follows since, in the commutative case, the Brown-McCoy radical and the Jacobson radical ([3], [5]) agree.

2.5 Lemma. *Let A be an algebra over the complex field with (Jacobson) radical R. Let R_1 be its radical when A is considered as an algebra over the real field. Then $R = R_1$.*

It is clear from the definitions ([3], p. 476) that $R \subset R_1$. Let $x \varepsilon R_1$, c real, $\neq 0$. Then cx^2 has an adverse in A. This shows that cix has an adverse in A, for otherwise $-i/c$ is in the spectrum of x ([3], p. 458) and $-c^{-2}$ is in the spectrum of x^2 which is impossible. Let $\alpha = a + bi$, a, b real, be any complex number. Let r be the adverse of bix. Using the notation $t_1 \circ t_2 = t_1 + t_2 - t_1 t_2$, we have, by [3], p. 477, for any $s \varepsilon A$,

$$[bix + (ax + yx)] \circ (r \circ s) = [ax + yx - (ax + yx)r] \circ s.$$

Now $ax + yx - (ax + yx)r \varepsilon R_1$ and thus has a right adverse s. This shows that $\alpha x + yx$ has a right adverse. Similar arguments ([3], p. 477) show that $\alpha x + yx$ has a left adverse. Thus $x \varepsilon R$.

This shows that the results of Section 4 concerning semi-simple real Banach algebras hold for semi-simple complex Banach algebras.

3. Examples. We indicate one way in which our mappings of period $n > 2$ can behave differently from those of period 2. First consider the following easy result where T is an automorphism or anti-automorphism of finite period on a real Banach algebra B.

3.1. LEMMA. *T is continuous on B if and only if H_1 and K_1 are closed and T is continuous on K_1.*

Define for $x = u + v$, $u \,\varepsilon\, H_1$, $v \,\varepsilon\, K_1$ a new norm $\| x \|_1 = \| u \| + \| v \|$. If H_1 and K_1 are closed this is readily seen to be a complete Banach space norm for B. Since $\| x \|_1 \geqq \| x \|$, the two norms give the same topology for B by [1], p. 41. Next assume that T is continuous on K_1. There is a constant $c > 0$ such that $\| T(v) \| \leqq c \| v \|$, $v \,\varepsilon\, K_1$. Then, for $x = u + v$, as above,

$$\| T(x) \|_1 = \| u \| + \| T(v) \| \leqq (1 + c) \| x \|_1$$

which gives the continuity of T.

Note that the continuity of T on K_1 is automatic if the period of T is two, for then $T(x) = -x$, $x \,\varepsilon\, K_1$. However if the period exceeds two it is possible, as the following example shows, to have H_1, K_1 closed while T is not continuous on K_1.

Let B be the complex L_p space on the unit interval where $p > 1$ and $p \neq 2$. We consider B as a zero algebra. As is well-known [8] there exists a closed complex linear manifold M in B on which there exists no continuous complex-linear projection of B. Let N be a complex linear manifold which is a complementary manifold to M. For $x = u + v$, $u \,\varepsilon\, M$, $v \,\varepsilon\, N$ define T by the rule $T(x) = \omega u + \omega^2 v$ where ω and ω^2 are the non-real cube roots of unity. It is easy to check that T is linear on B and that $I + T + T^2 = 0$. Then $T^3 = I$ and T is periodic. Here $K_1 = B$ and $H_1 = (0)$.

Now N is not closed for otherwise, [8], Lemma 1.1.1, there exists a continuous complex-linear projection of B on M. Let $x_0 \,\varepsilon\, \bar{N}$, $x_0 \not\varepsilon\, N$, $x_0 = u_0 + v_0$, $u_0 \,\varepsilon\, M$, $v_0 \,\varepsilon\, N$. Then $u_0 \neq 0$, $u_0 \,\varepsilon\, M \cap \bar{N}$. Let $v_n \,\varepsilon\, N$, $v_n \to u_0$. We have $T(v_n) = \omega^2 v_n \to \omega^2 u_0$ while $T(u_0) = \omega u_0$. Thus T is discontinuous.

Next we show that H_1 can be closed with K_1 not closed. In this example we do not use a zero algebra. Let B be the L_p space considered above with, however, a different rule for multiplication. Let f be a linear functional on B, $\| f \| = 1$ such that f vanishes on M. Select $W \,\varepsilon\, M$, $\| w \| = 1$. Define the product in B by the rule $x_1 x_2 = f(x_1) f(x_2) w$. It is easy to verify that this definition makes B into a commutative Banach algebra. Consider the mapping $x \to x^*$ defined by the rule that if $x = u + v$, $u \,\varepsilon\, M$, $v \,\varepsilon\, N$ then $x^* = u - v$. This mapping is an automorphism of B of period two. We have $H = M$,

$K = N$ and thus H is closed whereas K is not. Using these ideas an example can also be given where K is closed and H is not. As shown in Section 4 this type of behavior cannot take place if B is semi-simple.

4. The separating ideal and continuity for T. Henceforth T will represent a periodic automorphism or anti-automorphism with finite period on a real Banach algebra B with separating ideal S.

4.1. LEMMA. (1) $S \subset \bar{K}_1$. (2) $T(S) = S$. (3) *If* $u + v \varepsilon S$ *where* $u \varepsilon H_1$, $v \varepsilon K_1$ *then* $u \varepsilon S$ *and* $v \varepsilon S$. (4) $S = S \cap H_1 \oplus S \cap K_1$.

(1). Let $y \varepsilon S$, $x_k \to y$, $T(x_k) \to 0$. Set $x_k = u_k + v_k$ where $u_k \varepsilon H_1$ and $v_k \varepsilon K_1$. Then $u_k + T(v_k) \to 0$. This shows that $v_k - T(v_k) \to y$. But $v_k - T(v_k) \varepsilon K_1$ by Lemma 2.1.

(2). Since $T^{n-1} = T^{-1}$, where n is the period of T, it is enough to show that $T(S) \subset S$. Let $y = u + v \varepsilon S$ where $u \varepsilon H_1$, $v \varepsilon K_1$. Adopt the notation of the proof of (1). Since $u_k + v_k \to u + v$ and $u_k + T(v_k) \to 0$, we have $(u - u_k) + (v - v_k) \to 0$ and $T[(u - u_k) + (v - v_k)] \to u + T(v) = T(y)$. Thus $T(y) \varepsilon S$.

(3). By (2), $P_n(S) \subset S$. Thus, in the above notation, $P_n(y) = u \varepsilon S$. Then also $v = y - u \varepsilon S$.

(4). This follows from (3).

Below the notation Q' is used for the derived set of Q.

4.2. LEMMA. *Let T have period n on B. Then*

(a) $H_1' \cap K_1 \subset S$.

(b) *n even, T^2 continuous on $\bar{K}_1$ imply that* $K_1' \cap H_1 \subset S$.

(c) *$n = 2$ implies that* $S = H_1' \cap K_1 \oplus K_1' \cap H_1$.

(a). Let $u_k \varepsilon H_1$, $u_k \to v$, $v \varepsilon K_1$. Then $u_k - v \to 0$ and $T(u_k - v) \to v - T(v)$. Thus $v - T(v) \varepsilon S$. Then, by Lemma 4.1, $T^i(v) - T^{i+1}(v) \varepsilon S$, $i = 0, 1, 2, \cdots$. Also

$$\sum_{m=0}^{n-1} \sum_{i=0}^{m} [T^i(v) - T^{i+1}(v)] = \sum_{m=0}^{n-1} [v - T^{m+1}(v)] = nv.$$

Therefore $v \varepsilon S$.

(b). Let $v_k \varepsilon K_1$, $v_k \to u$, $u \varepsilon H_1$. Set $W = I + T^2 + T^4 + \cdots + T^{n-2}$. Then $TW(v_k) = -W(v_k)$. Also $W(v_k) \to (n/2)u$. Then $(n/2)u + W(v_k) \to nu$, $T[(n/2)u + W(v_k)] \to 0$. Thus $u \varepsilon S$.

(c). The conclusions (a) and (b) show that here

$$H_1' \cap K_1 \oplus K_1' \cap H_1 \subset S.$$

Let $y \varepsilon S$. Then there exist sequences $\{u_k\}$ and $\{v_k\}$ in H_1 and K_1 respectively such that $u_k + v_k \to y$, $u_k - v_k \to 0$. Thus $y/2 = \lim u_k = \lim v_k$. Via Lemma 4. 1, $S = S \cap H_1 \oplus S \cap K_1 \subset K_1' \cap H_1 \oplus H_1' \cap K_1$.

4. 3. THEOREM.

(a) *If $S \subset H_1$ then H_1 is closed and S is a zero algebra.*

(b) *If H_1 is closed and T is continuous on K_1 then $S \subset H_1$.*

(a). Let $v \varepsilon H_1' \cap K_1$. By Lemma 4. 2, $v \varepsilon S \subset H_1$. Thus $v \varepsilon H_1 \cap K_1 = (0)$. *Apply Theorem* 2. 4.

(b). Let n be the period of T. In view of Lemma 4. 1 it is enough to show that $S \cap K_1 = (0)$. Let $y \varepsilon S \cap K_1$, $u_k \varepsilon H_1$, $v_k \varepsilon K_1$ where $u_k + v_k \to y$ and $u_k + T(v_k) \to 0$. Then $v_k - T(v_k) \to y$. By Lemma 2. 1, $T^i(v_k) - T^{i+1}(v_k) \varepsilon K_1$, $T^i(y) \varepsilon K_1$. By the continuity of T on K_1 we obtain

$$T^i(v_k) - T^{i+1}(v_k) \to T^i(y), \qquad i = 0, 1, 2, \cdots. \tag{1}$$

But, as in the proof of Lemma 4. 2,

$$\sum_{m=0}^{n-1} \sum_{i=0}^{m} [T^i(v_k) - T^{i+1}(v_k)] = nv_k. \tag{2}$$

From (1) and (2) it follows that

$$nv_k \to \sum_{m=0}^{n-1} \sum_{i=0}^{m} T^i(y) = ny + \sum_{m=1}^{n-1} (n-m) T^m(y) \tag{3}$$

$= w$, say. Then $nu_k \to ny - w \varepsilon K_1$. Since H_1 is closed, $w = ny$. This gives

$$\sum_{m=1}^{n-1} (n-m) T^m(y) = 0. \tag{4}$$

Operating on this by T^{-1} we obtain

$$\sum_{m=0}^{n-2} (n-m-1) T^m(y) = 0. \tag{5}$$

Subtracting (4) from (5) we have

$$0 = (n-1)y - \sum_{m=1}^{n-1} T^m(y) = ny. \tag{6}$$

This completes the proof.

4. 4. LEMMA. *Let T have even period n with separating ideal S. Let S_1 be the separating ideal for T on S. Then*

(a) *$S \subset K_1$ and T^2 continuous on $S(\bar{K}_1)$ imply that $S_1 \subset K_2$ (K_1 closed).*

(b) *If, in addition, $n = 2$ (4) then $S(S_1)$ is a zero algebra.*

(a). Let n be the period of T. Suppose $y \varepsilon S_1$. Then there exists a sequence $\{v_k\} \subset S$, $v_k \to y$, $T(v_k) \to 0$. By the continuity of T^2 on S we obtain $T^i(v_k) \to T^i(y)$ or zero according as i is even or odd. Then, since $v_k \varepsilon K_1$, $(I + T^2 + \cdots + T^{n-2})(y) = 0$ or $y \varepsilon K_2$.

Now suppose that T^2 is continuous on $\bar{K}_1$. By Lemma 4.2, $K_1' \cap H_1 \subset S \subset K_1$. Thus $K_1' \cap H_1 = (0)$.

(b). If $n = 2$, then since here $K_2 = (0)$, S is a zero algebra by Theorem 2.4. If $n = 4$, then T^2 is an automorphism of period two and, for $x, y \varepsilon S_1$, $-xy = T^2(xy) = T^2(x)T^2(y) = xy$.

The following algebraic result may have some independent interest.

4.5. LEMMA. *Let B be a semi-simple algebra where T is an automorphism of period 2^n, $n = 0, 1, 2, \cdots$. Then H_1 is a semi-simple algebra.*

Since T is an automorphism, H_1 is a sub-algebra of B. The proof is by induction. If $n = 0$ then $H_1 = B$ and the conclusion trivial. Suppose that the conclusion holds for n. Let T have period 2^{n+1}. Then T^2 has period 2^n. By induction hypothesis, H_2 is semi-simple. If $H_2 = H_1$ we are through. Otherwise consider the decomposition $H_2 = H_1 \oplus H_2 \cap K_1$ provided by Lemma 2.2 where $H_2 \cap K_1 = \{x \varepsilon B \mid T(x) = -x\}$. T has period two as an automorphism defined on H_2. Let x be in the radical R of H_1. Then $\alpha x + yx$ has an adverse (reverse) in H_1 for all scalars α and all $y \varepsilon H_1$ (see [3], Chapter 22). Consider $z \varepsilon H_2 \cap K_1$. It is easy to see that $(zx)^2$ and $zxz \varepsilon H_1$. Thus $(zx)^2 \varepsilon R$. Using the notation $t_1 \circ t_2 = t_1 + t_2 - t_1 t_2$ we have, for every $s \varepsilon B$ the identities

$$(zx) \circ [(-zx) \circ s] = (zx)^2 \circ s, \qquad [s \circ (-zx)] \circ (zx) = s \circ (zx)^2.$$

If s is taken as the adverse of $(zx)^2$ in H_1 it follows from [3], p. 456, that $(-zx) \circ s$ is the adverse of zx. Moreover since $-zx \varepsilon H_2 \cap K_1$, this adverse lies in H_2.

Let $w = u + v$, $u \varepsilon H_1$, $v \varepsilon H_2 \cap K_1$ be any element of H_2 and let α be any scalar. $\alpha x + ux$ has an adverse p in H_1 since $x \varepsilon R$. Since $x - xp \varepsilon R$ then $v(x - xp)$ has an adverse q in H_2 by the above. But then (see [3], p. 477) we have, where $\alpha x + wx = (\alpha x + ux) + vx$, the relation

$$(\alpha x + wx) \circ (p \circ q) = (vx - vxp) \circ q = 0.$$

Also $v - pv \varepsilon H_2 \cap K_1$ so that $(v - pv)x$ has an adverse q_1 in H_2 and $(q_1 \circ p) \circ (\alpha x + wx) = 0$. Thus x lies in the radical of H_2. Hence H_1 is semi-simple and the induction is complete.

As applied to an anti-automorphism T of period 2^n on B this result gives the semi-simplicity of H_2.

4. 6. THEOREM. *Let B be a semi-simple Banach algebra. Then any T with period 2^n defined on B such that its separating ideal $S \subset K_1$ (as when K_1 is closed) is continuous.*

If $n = 1$ then $T^2 = I$ and S is a zero algebra by Lemma 4. 4 so the result holds for $n = 1$ by the semi-simplicity of B. For $n > 1$ we argue as follows. We show, by induction, that $S \subset K_{2^i}$ for $i = 0, 1, \cdots, n$. This is true for $i = 0$ by assumption. Suppose it is true for i, $0 \leqq i < n$. Now $H_{2^{i+1}}$ is semi-simple (Lemma 4. 5). Also $H_{2^{i+1}} \cap K_{2^i} = \{x \varepsilon B \mid T^{2^i}(x) = -x\}$ by Lemma 2. 2. Let $J = S \cap H_{2^{i+1}}$. J is a two-sided ideal in $H_{2^{i+1}}$. Let $u_k \varepsilon J$, $k = 1, 2$. Then $u_1 u_2 \varepsilon J$. If $i = 0$, $T^{2^i} = T$ may be either an automorphism or anti-automorphism. If $i > 0$, T^{2^i} is an automorphism. We have then either $-u_1 u_2 = T^{2^i}(u_1 u_2) = u_1 u_2$ or $-u_1 u_2 = u_2 u_1$. In any case $x^2 = 0$, $x \varepsilon J$. Thus J is contained in the radical of $H_{2^{i+1}}$ and therefore $J = (0)$. Set $V = T^{2^{i+1}}$. By Lemma 4. 1, $V(S) = S$. The period of V is $2^{n-i-1} = r$. Arguing as in Lemma 4. 1 (3) and (4) and using P_r we have that

$$S = S \cap H_{2^{i+1}} \oplus S \cap K_{2^{i+1}} = S \cap K_{2^{i+1}}.$$

Thus $S \subset K_{2^{i+1}}$. However $K_{2^n} = (0)$ whence T is continuous.

4. 7. THEOREM. *Let B be a semi-simple Banach algebra. Suppose that every automorphism and anti-automorphism with period two on each closed semi-simple Banach sub-algebra B_1 of B is continuous, at least for B_1 where there is a continuous projection of B on B_1. Then every T of period 2^n on B is continuous, $n = 1, 2, \cdots$.*

The proof is by induction. The case $n = 1$ is clear. Suppose that the result holds for n and that T has period 2^{n+1}. Now by assumption, T^2 is continuous. Thus H_2 and K_2 are closed. Since $B = H_2 \oplus K_2$ it follows from [8], Lemma 1. 1. 1, that there is a continuous projection of B on H_2. H_2 is semi-simple by Lemma 4. 5. Thus T is continuous on H_2 since T has period one or two on H_2. Since $H_2 = H_1 \oplus H_2 \cap K_1$ and $H_2 \cap K_1 = \{x \varepsilon B \mid T(x) = -x\}$ by Lemma 2. 2, then $H_2 \cap K_1$ is closed. Also from Lemma 2. 2, $K_1 = K_2 \oplus H_2 \cap K_1$. By [7], p. 220, K_2 and $H_2 \cap K_1$ are disjoint closed linear manifolds and K_1 is closed. Then $S \subset K_1$ in view of Lemma 4. 1. The continuity of T now follows from Theorem 4. 6.

4. 8. COROLLARY. *Let B satisfy the conditions of Theorem 4. 7. Suppose*

that every automorphism of period k defined on B is continuous where k is an odd number. Then every T defined on B with period $2^n k$ is continuous, $n = 0, 1, 2, \cdots$.

For $n = 0$ we consider T an anti-automorphism of period k. Since k is odd it follows readily that such T can exist only if B is commutative. Then the continuity of T follows from [10], Corollary 6. 3.

Let T have period $2k$. Then T^2 is a continuous automorphism with period k. Let $k = 2r + 1$. T^k is continuous by Theorem 4. 7. Then so is $T = T^k T^{-2r}$.

Suppose that every T of period $2^{n-1}k$ is continuous where $n > 1$. Let T have period $2^n k$. Then T^2 is continuous. Arguing as above, we obtain the continuity of T. The result now follows by induction.

4. 9. LEMMA. *Let T have period three where H_1 and K_1 are closed and K_1 is a sub-algebra of B. Then S is a zero algebra.*

Since $B = H_1 \oplus K_1$ and H_1, K_1 are closed then ([7], p. 220) there exist constants $c_1, c_2 > 0$ such that, for $x = u + v$, $u \, \varepsilon \, H_1$, $v \, \varepsilon \, K_1$, $\| u \| \leqq c_1 \| x \|$ and $\| v \| \leqq c_2 \| x \|$. Let $x_i \, \varepsilon \, S$, $x_n^{(i)} \to x_i$, $x_n^{(i)} = u_n^{(i)} + v_n^{(i)}$, $u_n^{(i)} \, \varepsilon \, H_1$, $v_n^{(i)} \, \varepsilon \, K_1$ and $u_n^{(i)} + T(v_n^{(i)}) \to 0$, $i = 1, 2$. By Lemma 4. 1, $x_i \, \varepsilon \, K_1$. Also $\| v_n^{(i)} - x_i \| \leqq c_2 \| u_n^{(i)} + (v_n^{(i)} - x_i) \| \to 0$. Then $u_n^{(i)} \to 0$, $v_n^{(i)} \to x_i$ and $T(v_n^{(i)}) \to 0$. Since $I + T + T^2 = 0$ on K_1 and T^2 is an automorphism.

$$T^2(v_k^{(1)} v_k^{(2)}) = - v_k^{(1)} v_k^{(2)} - T(v_k^{(1)} v_k^{(2)}),$$

$$T^2(v_k^{(1)} v_k^{(2)}) = [v_k^{(1)} + T(v_k^{(1)})][v_k^{(2)} + T(v_k^{(2)})].$$

This gives

$$\begin{aligned} -2v_k^{(1)} v_k^{(2)} - T(v_k^{(1)} v_k^{(2)}) - T(v_k^{(1)}) T(v_k^{(2)}) \\ = v_k^{(1)} T(v_k^{(2)}) + T(v_k^{(1)}) v_k^{(2)}. \end{aligned}$$

Whether T is an automorphism or an anti-automorphism we obtain in the limit that $x_1 x_2 = 0$.

4. 10. THEOREM. *Let B be semi-simple. Then any T defined on B with period three where $S \subset K_1$ is continuous.*

It is sufficient to show in view of Theorem 2. 4 that T is continuous on S. By Lemmas 4. 1 and 4. 9, the separating ideal S_1 of T on S is a zero algebra and is, furthermore, by Theorem 2. 4, a two sided ideal of B. Thus $S_1 = (0)$ and T is continuous.

For the notion of spectrum in a real Banach algebra see [6] and [10]. Here $\rho(x)$ denotes the spectral radius of $x = \sup | \alpha |$, for α in the spectrum of x.

4.11. LEMMA. *Let T have period two. Then for each $y \varepsilon H_1' \cap K_1$ $(K_1' \cap H_1)$ there exists a sequence $\{z_k\}$ in $H_1(K_1)$ such that $z_k \rightarrow y$, $\rho(z_k) \rightarrow 0$.*

Let $y \varepsilon H_1' \cap K_1(K_1' \cap H_1)$ and let $\{x_k\}$ be a sequence in $H_1(K_1)$ such that $x_k \rightarrow y$. Set $w_k = (x_k + y)/2$. Then $w_k \rightarrow y$ and $w_k \varepsilon \bar{H}_1(\bar{K}_1)$. By a theorem of Hille, [3], Theorem 22.9.1, for each integer k there exists an element z_k in $H_1(K_1)$ such that simultaneously $\| w_k - z_k \| < k^{-1}$, $0 \leqq \rho(z_k) < \rho(w_k) + k^{-1}$. Note that

$$\rho(w_k) = \rho[T(w_k)] \leqq \| T(w_k) \| = \| x_k - y \|/2 \rightarrow 0.$$

Then we have $z_k \rightarrow y$ and $\rho(z_k) \rightarrow 0$.

4.12. LEMMA. *Let T have period two on B. Suppose that $x_k \varepsilon H$, $k = 1, 2, \cdots, x_k \rightarrow x$, $x \varepsilon H$ and $\rho(x_k) \rightarrow 0$ imply that $x = 0$. Then K is closed. The condition on H is fulfilled if there exists a sub-additive function $| x |$ defined on H vanishing only for $x = 0$ such that $0 \leqq | x | \leqq \rho(x)$, $x \varepsilon H$.*

To show K closed it is sufficient to show that $K' \cap H = (0)$. Let $y \varepsilon K' \cap H$. By Lemma 4.11 there exists a sequence $\{z_k\}$ in K such that $z_k \rightarrow y$ and $\rho(z_k) \rightarrow 0$. Then $z_k^2 \varepsilon H$, $z_k^2 \rightarrow y^2 \varepsilon H$ and $\rho(z_k^2) \rightarrow 0$. By hypothesis this gives $y^2 = 0 = \rho(y)$. Applying the hypothesis to the sequence $\{y, y, \cdots\}$ we obtain $y = 0$.

For the second statement note that if $x_k \varepsilon H$, $x_k \rightarrow x$, $x \varepsilon H$ and $\rho(x_k) \rightarrow 0$ then

$$| x | \leqq | x - x_k | + | x_k | \leqq | x - x_k | + \rho(x_k) \rightarrow 0.$$

This gives $x = 0$.

If T is the involution in an A^*-algebra [10] or in a ρ^*-algebra [11], then such a sub-additive function exists on H.

The next result gives conditions under which all repeated square roots of a continuous automorphism are continuous.

4.13. THEOREM. *Let B be semi-simple and let T have period two satisfying the condition of Lemma 4.12. Then any automorphism or anti-automorphism U of B such that $U^{2^n} = T$ is continuous, $n = 0, 1, 2, \cdots$.*

The case $n = 0$ is disposed of by Lemma 4.12 and Theorem 4.6. Suppose that the result holds for $n - 1$. Let $U^{2^n} = T$. Then U^2 is continuous. This gives the closure of H_2 and K_2 computed for U. Moreover H_2 is semi-simple by Lemma 4.5. We show that U is continuous on H_2. This is clear if $H_1 = H_2$; otherwise U has period two on H_2 (see arguments above, e.g. in Lemma 4.5). Since $H_1 \subset H$ (of T) the requirements of Lemma 4.12 are

fulfilled by U on the Banach algebra H_2. By the above U is continuous on H_2. Then $H_2 \cap K_1$ is closed. Arguing as in Theorem 4. 7, we see that K_1 is closed. Therefore U is continuous by Theorem 4. 6.

UNIVERSITY OF OREGON.

BIBLIOGRAPHY.

[1] S. Banach, *Théorie des opérations linéaires*, Monografje Matemacyzme, Warsaw (1932).

[2] B. Brown and N. H. McCoy, "Radicals and subdirect sums," *American Journal of Mathematics*, vol. 69 (1947), pp. 46-58.

[3] E. Hille, *Functional analysis and semi-groups*, American Mathematical Society Colloquium Publications, vol. 31, New York (1948).

[4] L. K. Hua, "On the automorphisms of a field," *Proceedings of the National Academy of Sciences*, vol. 35 (1949), pp. 386-389.

[5] N. Jacobson, "The radical and semi-simplicity for arbitrary rings," *American Journal of Mathematics*, vol. 67 (1945), pp. 300-320.

[6] I. Kaplansky, "Normed algebras," *Duke Mathematical Journal*, vol. 16 (1949), pp. 399-418.

[7] E. R. Lorch, "On a calculus of operators in reflexive vector spaces," *Transactions of the American Mathematical Society*, vol. 45 (1939), pp. 399-418.

[8] F. J. Murray, "On complementary manifolds and projections in the spaces L_p and l_p," *ibid.*, vol. 41 (1937), pp. 138-152.

[9] C. E. Rickart, "The singular elements of a Banach algebra," *Duke Mathematical Journal*, vol. 14 (1947), pp. 1063-1077.

[10] ———, "The uniqueness of norm problem for Banach algebras," *Annals of Mathematics*, vol. 51 (1950), pp. 615-628.

[11] B. Yood, "Topological properties of homomorphisms between Banach algebras," *American Journal of Mathematics*, vol. 76 (1954), pp. 155-167.

DE RHAM'S THEOREM FOR ARBITRARY SPACES.*

By J. Schwartz.

Introduction. The abstract axiomatic approach to homology of Eilenberg and Steenrod (see Eilenberg-Steenrod [2]) yields such powerful uniqueness theorems that most of the principal isomorphism theorems of homology and cohomology theory can be derived from the Eilenberg-Steenrod theorems as corollaries. One notable exception has been the isomorphism between topological cohomology (say of Čech type) and the special cohomology for differentiable manifolds which can be defined in terms of forms. The difficulty has been simply this: the Eilenberg-Steenrod method requires that cohomology groups be defined for all triangulable spaces, and not every triangulable space is a differentiable manifold. How to define forms on more general spaces than manifolds? Taking our clue from a fundamental property of differentiable manifolds, we make use of *imbeddings in Euclidean spaces.*

The definition of the appropriate groups of forms is given in Section 1, together with the quite simple proofs of the seven cohomology axioms of Eilenberg-Steenrod. The groups can be defined for arbitrary compact subsets of Euclidean space; i. e., we get a cohomology theory for arbitrary compact finite dimensional spaces. In Section 2, we obtain the relationship between our "extrinsic" groups of forms and the ordinary "intrinsic" groups of forms in the case that our space is a differentiable manifold. In Section 3 we obtain a generalization of de Rham's classical theorem in its original form as a theorem of duality. In Section 4 we discuss the case of non-triangulable spaces, showing that our groups are simply the Čech cohomology groups with real coefficients. In Section 5 we discuss the theory of open manifolds.

§1. Definition and Basic Properties of the de Rham Cohomology Groups. 1. Pairs of spaces imbedded in a Manifold. Let M be a C^∞ manifold (open or closed). Let S be a compact subset of M, and T a compact subset of S; so that (S, T) is a compact pair. We define spaces of forms as follows:

(a) $F_k(M)$ is the space of all C^∞ k-forms defined on M;

(b) $T_k(M; S)$ is the space of all C^∞ k-forms in $F_k(M)$ which vanish in a neighborhood of S;

* Received September 14, 1953.

(c) $Z_k(M; S, T) = \{f \varepsilon T_k(M; T) \mid df \varepsilon T_{k+1}(M; S)\}$;

(d) $F_k(M; S, T) = \{df + t \mid f \varepsilon T_{k-1}(M; T), t \varepsilon T_k(M, S)\}$.

We then put

$$H_k(M; S, T) = Z_k(M; S, T)/F_k(M; S, T).$$

The vector-space $H_k(M; S, T)$ may be called the k-th de Rham cohomology group of the pair S, T relative to the manifold M. We adopt the usual convention of taking all spaces to be zero-spaces for subscript $k < 0$. In this way, F_k, Z_k, T_k, and H_k are defined for all integer indices.

We shall show below that $H_k(M; S, T)$ is actually independent of M. For this reason, we begin our investigation by choosing some very large integer N, and supposing that all our spaces S, T are compact subsets of Euclidean space E^N. Wherever this is the case we will omit any specific notation for M in our notation. Thus we write $F_k(E^N)$ as F_k, $H_k(E^N; S, T)$ as $H_k(S, T)$, etc.

2. Mappings. Let $h: (S, T) \to (S_1, T_1)$ be a continuous mapping. Extend h to a continuous map $h': E^N \to E^N$. Let h_i be a sequence of C^∞ maps $E^N \to E^N$ which converge uniformly to h' on any compact subset of E^N. Then

LEMMA 1. *Let* $f \varepsilon Z_k(S_1, T_1)$. *Then, for sufficiently high* i, (a) $h_i^*f \varepsilon Z_k(S, T)$; (b) *the coset* $\operatorname{mod} F_k(S, T)$ *of* h_i^*f *is independent of* i. *We call this coset the limiting coset of* h_i^*f.

COROLLARY. *The limiting coset of* h_i^*f *is independent of the approximating sequence* h_i.

LEMMA 2. *The limiting coset of* h_i^*f *is independent of the particular extension* h' *of* h *chosen.*

The proofs of these lemmas are to be found in the appendix to this section.

LEMMA 3. *If* $f \varepsilon F_k(S_1, T_1)$, *then the limiting coset of* h_i^*f *is zero.*

Proof. $f = dg + t$, $g \varepsilon T_{k-1}(T_1)$ and $t \varepsilon T_k(S_1)$. It is clear from the definition that $h_i^*g \varepsilon T_{k-1}(T)$ and $h_i^*t \varepsilon T_k(S)$ for all sufficiently large i. This shows, however, that $h_i^*f = dh_i^*g + h_i^*t$ is in $F_k(S, T)$ for sufficiently large i, so that the limiting coset of h_i^*f is zero.

Definition 1. If $g \varepsilon H_k(S_1, T_1)$, and z is an element of the coset g, we put $h^*g =$ limiting coset of h_i^*z. Lemmas 1, 2, and 3 ensure that this

is a single-valued definition. It is clear that $h^*: H_k(S_1, T_1) \to H_k(S, T)$ is a linear map.

LEMMA 4. *If* $h: (S, T) \to (S_1, T_1)$, *and* $h_1: (S_1, T_1) \to (S_2, T_2)$, *then* $(h_1 h)^* = h^* h_1^*$.

Proof. Let h' and h_1' be extensions of h and h_1 to all of E^N. Let h_i and $h_i^{(1)}$ be sequences of C^∞ maps which converge uniformly on any compact set to h' and h_1', respectively. Then $h_i^{(1)} h_i$ is a sequence of C^∞ maps which converge uniformly on any compact set to $h_1' h'$, which is an extension of $h_1 h$. If $g \,\varepsilon\, H_k(S_2, T_2)$, and z is an element of the coset g, $(h_1 h)^* g =$ limiting coset of $(h_i^{(1)} h_i)^* z =$ limiting coset of $h_i^*(h_i^{(1)} z)$. From the fact that the limiting coset of $h_i^{(1)} z$ is $h_1^* z$, and from Lemma 3, the equation $(h_1 h)^* g = h^* h_1 g$ follows readily.

LEMMA 5. *If i is the identity map* $i: (S, T) \to (S, T)$, *then* $i^*: H_n(S, T) \to H_n(S, T)$ *is the identity map.*

Proof. As an extension of i we take i', the identity map of E^N. Then we can approximate i' by $h_j = i'$; it follows that each h_j^* is an identity map, so i^* is also an identity map.

LEMMA 6. *Suppose that U is a relatively open subset of S, and that the closure of U and the closure of $S - T$ are disjoint, i.e.* $\mathrm{cl}(U) \cap \mathrm{cl}(S - T) = \varnothing$. *Let i be the natural identity map of* $(S - U, T - U) \to (S, T)$. *Then*

$$i^*: H_n(S, T) \to H_n(S - U, T - U)$$

is an isomorphism onto.

Proof. (A) i^* is onto. Let $z \,\varepsilon\, Z_k(S - U, T - U)$. Since $\mathrm{cl}(U) \cap \mathrm{cl}(S - T) = \varnothing$, we can find a C^∞ function f defined on all of E^n, such that $f \equiv 1$ on a neighborhood of $\mathrm{cl}(S - T)$; $f \equiv 0$ on $\mathrm{cl}(U)$. Then (1) $f \wedge z = 0$ near $\mathrm{cl}(U)$ and near $T - U$, i.e., $f \wedge z \,\varepsilon\, T_k(T)$. (2) $d(f \wedge z) = df \wedge z + f \wedge dz$. We have $dz = 0$ near $S - U$, $f = 0$ near $\mathrm{cl}(U)$, so the second term of this expression is in $T_{k+1}(S)$. We have $df = 0$ near $\mathrm{cl}(U) \cap \mathrm{cl}(S - T)$, and $z = 0$ near $T - U$, so that the first term $df \wedge z$ is in $T_{k+1}(S)$. Taking all together, we see that $f \wedge z \,\varepsilon\, Z_k(S, T)$. (3) Write $z' = f \wedge z$. Then $z - z' = (1 - f) \wedge z$. Since $1 - f \equiv 0$ near $\mathrm{cl}(S - T)$, and $z \equiv 0$ near $T - U$, we have $z - z' \,\varepsilon\, T_k(S - U)$, so $z - z' \,\varepsilon\, F_k(S - U, T - U)$. Thus, z' and z belong to the same class ν in $H_k(S - U, T - U)$. If ν' is the class in $H_k(S, T)$ which contains z', it is

clear that $i^*\nu' = \nu$. Since z was an arbitrary element of $Z_k(S-U, T-U)$, we have proved i^* is onto.

(B) i^* is one-to-one. For, let $\nu \varepsilon H_k(S, T)$, and suppose that $i^*\nu = 0$. Then, if $z \varepsilon Z_k(S, T)$ belongs to the class ν, it follows that

$$z = dg + t, \qquad g \varepsilon T_{k-1}(T-U), \qquad t \varepsilon T_k(S-U).$$

Since $z \equiv 0$ near T, it follows that $dg = -t$ near T. We then choose a C^∞ function f as in part (A) of the proof of this lemma, and write

$$z = d(f \wedge g) + (1-f) \wedge dg - df \wedge g + f \wedge t + (1-f) \wedge t;$$

since $f = 0$ near $\mathrm{cl}(U)$, and $g = 0$ near $T - U$, $f \wedge g \varepsilon T_{k-1}(T)$, and we have only to show that

$$m = (1-f) \wedge dg - df \wedge g + f \wedge t + (1-f) \wedge t \varepsilon T_k(S)$$

to prove that $z \varepsilon F_k(S, T)$, so that $\nu = 0$. Now, near T, m is $f \wedge t - df \wedge g$. We have $df = 0$ near $\mathrm{cl}(U)$, $g = 0$ near $T - U$; $f = 0$ near U, $t = 0$ near $S - U$; hence $m = 0$ near T. Near $\mathrm{cl}(S-T)$ we have $(1-f) \equiv 0$, so that $m = f \wedge t - df \wedge g$ once more. Since t and df are zero near $\mathrm{cl}(S-T)$, $m = 0$ near $\mathrm{cl}(S-T)$. Altogether $m = 0$ near S, so that $m \varepsilon T_k(S)$.

3. The boundary operator. From the definitions of the various spaces it is clear that (a) $d: F_k(T) \to K_{k+1}(S, T)$, (b) $d: Z_k(T) \to Z_{k+1}(S, T)$. Thus, d defines a natural map $d^*: H_k(T) \to H_{k+1}(S, T)$ by passage to factor groups.

Once d^* is defined, we can follow Eilenberg-Steenrod by letting $j: T \to S$ and $i: S \to (S, T)$ be the natural identity maps, and considering the "homology" sequence of groups and homomorphisms

$$\cdots \xleftarrow{i^*} H_{k+1}(S, T) \xleftarrow{d^*} H_k(T) \xleftarrow{j^*} H_k(S) \xleftarrow{i^*} H_k(S, T) \xleftarrow{d^*} \cdots.$$

LEMMA 7. *The homology sequence is exact.*

Proof. (a_1) If ν is an element of $H_k(T)$, and $z \varepsilon Z_k(T)$ is in the class ν, then $i^*d^*\nu$ is evidently the class in $H_{k+1}(S)$ of dz. Since $dz \varepsilon F_{k+1}(S)$, $i^*d^*\nu = 0$.

(b_1) If ν is an element of $H_k(T)$, and $z \varepsilon Z_k(S)$ is in the class ν, then $d^*j^*\nu$ is evidently the class in $H_{k+1}(S, T)$ of dz. Since $dz \varepsilon T_{k+1}(S)$, $d^*j^*\nu = 0$.

(c_1) If ν is an element of $H_k(S, T)$, and $z \varepsilon Z_k(S, T)$ is in the class ν, then $j^*i^*\nu$ is evidently the class in $H_k(T)$ of z. Since $z \varepsilon T_k(T) \subseteq F_k(T)$, it follows that $j^*i^*\nu = 0$.

(a_2) Let $\nu \varepsilon H_k(T)$, $d^*\nu = 0$. If $z \varepsilon Z_k(T)$ is in the class ν, it follows that $dz \varepsilon F_{k+1}(S, T)$, so that $dz = dz_1 + z_2$, $z_1 \varepsilon T_k(T)$, $z_2 \varepsilon T_{k+1}(S)$. I. e., $d(z - z_1) \varepsilon T_{k+1}(S)$; $z - z_1 \varepsilon Z_k(S)$. Thus the class $\nu' \varepsilon H_k(T)$ of $z - z_1$ is in $j^*H_k(S)$. Since $z_1 \varepsilon T_k(T) \subseteq F_k(T)$, $\nu = \nu'$.

(b_2) Let $\nu \varepsilon H_k(S)$, $j^*\nu = 0$. If $z \varepsilon Z_k(S)$ is in the class ν, it follows that $z \varepsilon F_k(T)$; i. e., $z = dz_1 + z_2$, $z_1 \varepsilon F_k$, $z_2 \varepsilon T_k(T)$. Thus $z - dz_1 \varepsilon T_k(T)$; so that $z - dz_1 \varepsilon Z_k(S, T)$. If ν' is the class in $H_k(S)$ of $z - dz_1$, it follows that $\nu' \varepsilon i^*H_k(S, T)$. But, since $dz_1 \varepsilon F_k(S)$, $\nu' = \nu$.

(c_2) Let $\nu \varepsilon H_k(S, T)$, $i^*\nu = 0$. If $z \varepsilon Z_k(S, T)$ is an element of the class ν, it follows that $z \varepsilon F_k(S)$; i. e., $z = dz_1 + z_2$, $z_1 \varepsilon F_{k-1}$, $z_2 \varepsilon T_k(S)$. Then $z - z_2 = dz_1$; since $z - z_2 \varepsilon T_k(T)$, $z_1 \varepsilon Z_{k-1}(T)$. It follows that the class ν' of $z - z_2$ in $H_k(S, T)$ is in $d^*H_{k-1}(T)$; since $z_2 \varepsilon T_k(T) \subseteq F_k(T)$, $\nu' = \nu$.

LEMMA 8. *Let $h: (S, T) \to (S_1, T_1)$ be a continuous map, and let $h_1: T \to T_1$ be its restriction to T. If $\nu \varepsilon H_{k-1}(T_1)$, then $d^*h_1^*\nu = h^*d^*\nu$.*

Proof. Let h' be an extension of h to all of E^N, and let h_i be a sequence of C^∞ maps of $E^N \to E^N$ which converge uniformly to h' on every compact set. Then, if $z \varepsilon Z_{k-1}(T)$, $h^*d^*\nu =$ limiting coset in $H_k(S, T)$ of h_i^*dz $=$ limiting coset in $H_k(S, T)$ of dh_i^*z. Since the limiting coset of h_i^*z is $h_1^*\nu$, our lemma is now evident.

LEMMA 9. *Let $h_0, h_1: (S, T) \to (S_1, T_1)$ be continuons maps which are homotopic. Then $h_0^* = h_1^*$.*

LEMMA 10. *Let z be a k-form such that $dz \equiv 0$ near a point p, $k > 1$. Then we can find a form z_1 such that $z \equiv dz_1$ near p.*

These lemmas are proved in the appendix to this section. Lemma 10 evidently implies: If P is a one point space, $H_k(P) = 0$ for $k > 0$. In dimension 0, $Z_0(P)$ is the space of all scalar functions constant near P, and $F_0(P) = T_0(P)$ is the space of all scalar functions zero near P. Thus $H_0(P)$ is isomorphic with the field of real numbers.

We have now verified all properties of Eilenberg-Steenrod, and can conclude that we have

THEOREM 1. *For every pair (S, T) of triangulable spaces, $H_k(S, T)$ is naturally isomorphic to the relative k-th cohomology group of (S, T), no matter how these cohomology groups are defined.*

4. Appendix. Homotopy properties of forms.

LEMMA 11. *Let M and N be C^∞ manifolds, and let f be a k-form on N. Suppose that $M \supseteq S \supseteq T$, where S and T are compact, and that we can define a map $h_t : M \to N$ for all $-1 < t < 2$ such that $h_t(m)$ is a C^∞ function both of the real variable t and of $m \in M$. If, for $0 \leqq t \leqq 1$,*

$$\text{(a)} \quad h_t(S) \cap \operatorname{car}(df) = \emptyset, \qquad \text{(b)} \quad h_t(T) \cap \operatorname{car}(f) = \emptyset,$$

then $h_0{}^*f$ and $h_1{}^*f$ are in the same coset of $Z_k(M; S, T)$ modulo $F_k(M; S, T)$.

Before giving the proof, we show how Lemma 11 implies Lemmas 1, 2, 9, and 10.

Proof of Lemma 1. Put $h_t{}^{(i,j)}(x) = th_i(x) + (1-t)h_j(x)$, and apply Lemma 11.

Proof of Lemma 2. Let h' and g' be two extensions of h, and let h_i approach h, g_i approach g, both uniformly on every compact set, where h_i and g_i are C^∞ maps. Put $h_t{}^{(i)}(x) = th_i(x) + (1-t)g_i(x)$, and apply Lemma 11.

Proof of Lemma 9. Let $h_t : (S, T) \to (S_1, T_1)$ be a continuous homotopy between h_0 and h_1. Extend h_t to a map $h_t' : E^N \to E^N$ which is defined and continuous for $-\infty < t < +\infty$, $x \in E^N$. Let $h_t{}^{(i)} : E^N \to E^N$ be a sequence of C^∞ maps depending in a C^∞ manner on the real parameter t, and such that $h_t{}^{(i)}$ approaches h_t' uniformly on every compact subset of E_n, uniformly for every bounded set of parameter values t. Let $z \in Z_k(S_1, T_1)$. Then $h_0{}^*z =$ limiting coset of $h_0{}^{(i)*}z$, $h_1{}^*z =$ limiting coset of $h_1{}^{(i)*}z$. Since, by Lemma 11, coset of $h_1{}^{(i)*}z =$ coset of $h_2{}^{(i)*}z$ for all sufficiently large i, Lemma 9 is proved.

Proof of Lemma 10. Put $h_t(x) = t(x-p) + p$. Then $h_1{}^*z = z$ and $h_0{}^*z = 0$ for every k-form z, $k > 0$. If $z \in Z_k(p)$, it follows by Lemma 11 that $z \in F_k(p)$; so from this, Lemma 10 is evident.

Proof of Lemma 11. We let I be the open interval $-1 < t < 2$, and let M' be the direct-product manifold $M \times I$. Define $H : M' \to N$ by $H[m, t] = h_t(m)$. Define $p : M' \to M$ by $p[m, t] = m$. Then inspection of the definitions reveals

$$(H^*f)[m, t] = p^*\{(h_t{}^*f)(m)\} + (p^*\beta_t{}^{(m)}) \wedge dt,$$

where β_t is a C^∞ $k-1$ form on M which depends in a C^∞ fashion on the real parameter t. From $h_t(T) \cap \operatorname{car}(f) = \emptyset$ it follows readily that $\operatorname{car}(\beta_t(m)) \cap T = \emptyset$. We have then

$$(H^*df)[m,t] = \pm\, \partial/\partial t p^*\{(h_t^*)(m)\} \wedge dt \pm p^*\{(h_t^*df)(m)\} + p^*d\beta_t \wedge dt.$$

Since $h_t(S) \cap \operatorname{car}(df) = 0$, $H^*df = 0$ near $S \times [0,1]$. Likewise, $h_t^*df = 0$ near $S \times [0,1]$. It follows that $\partial p^*(h_t^*f)/\partial t = \pm\, p^*(d\beta_t)$ or integrating from 0 to 1,

$$p^*(h_0^*f - h_1^*f \pm d\int_0^1 \beta_t dt) = 0; \text{ hence } h_0^*f - h_1^*f = \pm\, d\int_0^1 \beta_t dt.$$

Put $\pm \int_0^1 \beta_t dt = g$. Then $g \,\varepsilon\, T_{k-1}(T)$, so that $h_0^*f - h_1^*f \,\varepsilon\, F_k(S,T)$.

§2. Intrinsic Forms on a Manifold.

Definition 2. Let M be a C^∞ manifold. A C^∞ map $h: M \to E^N$ which determines a one-to-one map of the tangent vector space at every point on M is called a regular imbedding of M in E^N.

Definition 3. If, in Definition 2, M is a subset of E^N and the natural identity map $i: M \to E^N$ is a regular imbedding, we say that M is regularly imbedded in E^N.

LEMMA 12. *If M is a C^∞ manifold regularly imbedded in E^N, then there exists a neighborhood U and a map $n: U \to M$ such that the map $n: U \to M$ is a C^∞ retraction of U on M.*

Proof. We consider the C^∞ N-dimensional manifold Σ of segments $\sigma = [a,b]$ such that $a \,\varepsilon\, M$, and σ is orthogonal to M at its foot a. It is clear that the map $t: \Sigma \to E^N$ determined by $t[a,b] = b$ is a C^∞ map whose Jacobian determinant is non-zero at every point σ in the set of points Σ_0 of zero length. It follows by the implicit function theorem that there exists a neighborhood Φ of Σ_0 such that the map $t: \Phi \to E^N$ is C^∞, one-to-one, and maps onto an open set in E^N; t^{-1} is also C^∞ by the implicit function theorem. We can now put $s[a,b] = a$ and $n = st^{-1}$. Q. E. D.

Suppose that h is a regular imbedding of M in E^N. Put $\bar{S} = h(S)$, $\bar{T} = h(T)$. Then

$$h^*: Z_k(\bar{S}, \bar{T}) \to Z_k(M; S, T), \qquad h^*: F_k(\bar{S}, \bar{T}) \to F_k(M; S, T).$$

By passage to cosets we define, in the natural way, a map

$$h^*: H_k(\bar{S}, \bar{T}) \to H_k(M; S, T).$$

THEOREM 2. *If h is*

(a) *A regular imbedding of the manifold M,*

(b) *A non-singular linear map of the Euclidean space M, then h^* is an isomorphism onto.*

Proof. Without loss of generality, we can assume that M is regularly imbedded in E^N, and that h is the identity map of $M \to E^N$. Let n be the map whose existence is established in Lemma 12; $n: U \to M$, where U is a neighborhood of M. Suppose that $z \,\varepsilon\, Z_k(M; S, T)$. Then n^*z is defined and C^∞ in U. Let z_1 be a C^∞ form defined in all E^N such that $z_1 \equiv n^*z$ in a neighborhood of S. Then $z_1 \,\varepsilon\, Z_k(S, T)$, and $h^*z_1 = h^*n^*z = (nh)^*z = i^*z = z$ in a neighborhood of S. Thus, if $\nu \,\varepsilon\, H_k(M; S, T)$ is the coset of z, and $\nu' \,\varepsilon\, H_k(S, T)$ that of z_1, $\nu = h^*\nu'$; so that h^* is a mapping onto.

Conversely, suppose that $\nu' \,\varepsilon\, H_k(S, T)$, and that $h^*\nu' = 0$. If $z' \,\varepsilon\, Z_k(S, T)$ is an element of the class ν', it follows that $h^*z' = dg_1 + g_2$, $g_1 \,\varepsilon\, T_{k-1}(M; T)$, $g_2 \,\varepsilon\, T_k(M; S)$. Let g_1' and g_2', z'' be C^∞ forms defined on all of E^N such that $g_1' = n^*g_1$ near S, $g_2' = n^*g_2$ near S, $z'' = n^*h^*z'$ near S. Then $z'' = dg_1' + g_2' + g_3'$, where $g_1' \,\varepsilon\, T_k(T)$, $g_2' \,\varepsilon\, T_k(S)$, $g_3' \,\varepsilon\, T_k(S)$; so $z'' \,\varepsilon\, F_k(S, T)$. It only remains to show that $z'' - z' \,\varepsilon\, F_k(S, T)$, and this we do as follows:

Let $S_\epsilon = \{x \,\varepsilon\, E^N \mid |x - s| < \epsilon$ for some $s \,\varepsilon\, S\}$. The set U contains some set S_{ϵ_0}. Let $\eta = \frac{1}{2}\epsilon_0$, and put $H_t(m) = tm + (1-t)n(m)$, so that $H_t: S_\eta \to S_{\epsilon_0}$ for $-1 < t < 2$. The open sets S_{ϵ_0} and S_η can be regarded as manifolds. By Lemma 11, $H_0^*z' - H_1^*z' \,\varepsilon\, F_k(S_\eta; S, T)$. Now, it is easily seen that $H_0^*z' = n^*h^*z' = z''$ near S, and that $H_1^*z' = z$ near S. Thus $z'' - z' - dz_1 = 0$ near S, where z_1 is a suitably chosen form in $T_{k-1}(S_\eta; S, T)$. If z_1' is defined in all of E^N in such a way as to ensure $z_1 = z_1'$ near S, we have $z'' - z' - dz_1' = 0$ near S, so that $z'' - z' \,\varepsilon\, F_k(S, T)$.

§3. De Rham's theorem.

LEMMA 13. *Let H and $\mathfrak{H}$ be a cohomology and homology theory with coefficient-field equal to the field R of real numbers, both defined on an admissible category containing all triangulable pairs and their maps. Suppose that a bilinear multiplication (x, y) exists between elements of $H_n(A, B)$ and $\mathfrak{H}^n(A, B)$ such that*

(1) $(x, d_*y) = (d^*x, y)$ *for* $x \,\varepsilon\, H_{n-1}(B)$, $y \,\varepsilon\, \mathfrak{H}^n(A, B)$.

(2) $(x, j_*y) = (j^*x, y)$ *for* $x \,\varepsilon\, H_n(A_1, B_1)$, $y \,\varepsilon\, \mathfrak{H}^n(A, B)$, *and* $j: (A, B) \to (A_1, B_1)$ *an admissible map.*

(3) *The multiplication (x, y) between $H_0(P)$ and $H^0(P)$ is a dual pairing.*

Then the multiplication between $H_n(A,B)$ and $\mathfrak{h}^n(A,B)$ is a dual pairing for every triangulable pair.

Proof. We make use of Theorem III. 10. 1 of Eilenberg-Steenrod [2]. We introduce the space $H^n(A,B)$ of all linear functionals on $H_n(A,B)$, and let d_* and j_* be the linear maps of the spaces $H^n(A,B)$ dual to the corresponding maps d^*, j^* of $H_n(A,B)$. Then it is clear that the groups $H(A,B)$, and the maps d_* and j_* determine a homology theory. Now there exists a unique linear mapping $h: H^n(A,B) \to \mathfrak{h}^n(A,B)$ such that $(x, hy) = y(x)$ for $y \,\varepsilon\, H^n(A,B)$. In virtue of (1) and (2), this map has properties (2) and (3) of the Eilenberg-Steenrod Theorem III. 10. 1. In virtue of (3), the map $h: H^0(P) \to \mathfrak{h}^0(P)$ is an isomorphism onto. It then follows by the Eilenberg-Steenrod Theorem III. 10. 1 that $h: H^n(A,B) \to H^n(A,B)$ is an isomorphism onto for every triangulable pair. But this clearly means: the multiplication between $H_n(A,B)$ and $\mathfrak{h}^n(A,B)$ is a dual pairing for every triangulable pair. Q. E. D.

Let $\mathfrak{h}^n(A,B)$ denote the singular homology groups of the pair (A,B). In the particular case where (A,B) is a pair of open sets in Euclidean space, let $\mathfrak{h}_\infty{}^n(A,B)$ denote the relative singular groups based on C^∞ chains. Then there is a natural homomorphism $\tau: \mathfrak{h}_\infty{}^n(A,B) \to \mathfrak{h}^n(A,B)$. The map τ is an isomorphism onto. The absolute case of this result is well known; cf. Eilenberg [1]. The relative case results easily from the absolute by the use of the "five" lemma, Eilenberg-Steenrod [2], Lemma I. 4. 3. We can make use of these facts as follows. Let α be a relative singular cycle of a compact pair (A,B), where $A \subseteq E^N$. Let $z \,\varepsilon\, Z_n(A,B)$. Then we take a C^∞ cycle α_1 of $(E^N - \operatorname{car}(dz), E^N - \operatorname{car}(z)) = (U,V)$ which is in the same class of $h^n(U,V)$ as α. We put $(\alpha, z) = \int_{\alpha_1} z$. This multiplication is single-valued, since if α_2 is also a C^∞ cycle in the same class of $\mathfrak{h}^n(U,V)$ as α, then α_1 and α_2 are in the same class of $\mathfrak{h}_\infty{}^n(U,V)$, so that $\int_{\alpha_1} z = \int_{\alpha_2} z$ by Stoke's theorem. If α is in the zero class of $\mathfrak{h}^n(A,B)$, we may take $\alpha_1 = 0$, so that it follows that in this case, $(\alpha, z) = 0$. If $z \,\varepsilon\, F_n(A,B)$, then we can write $z = dz_1 + z_2$, $z_1 \,\varepsilon\, T_{n-1}(B)$, $z_2 \,\varepsilon\, T_{n-1}(A)$. We let $U_1 = E^N - \operatorname{car}(z_2)$; $V_1 = (E^N - \operatorname{car}(z_1)) \cap U_1$. Then we may suppose that α_1 is in the same class of $\mathfrak{h}^n(U_1, V_1)$ as α; in this case it follows by Stoke's theorem that

$$\int_{\alpha_1} (dz_1 + z_2) = \int_{\alpha_1} dz_1 = \int_{d\alpha_1} z_1 = 0.$$

Thus the multiplication (α, z) leads by passage to cosets to a multiplication

(h_1, h) between $\mathfrak{K}^n(A, B)$ and $H_n(A, B)$. Once we verify that this multiplication has the properties demanded in Lemma 13, we will have proved

THEOREM 3. *If (A, B) is a triangulable pair, then the multiplication between $\mathfrak{K}^n(A, B)$ and $H_n(A, B)$ introduced above is a dual pairing between these groups.*

If we now recall Theorem 2, and make use of the triangulation theorem for compact C^∞ manifolds and the isomorphism between the singular homology groups of such a manifold and the corresponding groups based on C^∞ chains (as given, say, in Eilenberg [1]), we can conclude

THEOREM 4. (*De Rham*). *Let S be a compact C^∞ manifold. Then* (a) *A closed form on S exists which has arbitrarily prescribed periods on independent cycles of S.*

(b) *If a closed form on S has period zero on every cycle of S, it is the exterior derivative of a form on S.*

To prove Theorems 3 and 4, we have, by Lemma 13, only to verify certain properties of the multiplication (h_1, h):

(1) Let $z \varepsilon Z_{n-1}(B)$, and let α be a singular cycle of A modulo B. Let $(U, V) = (E^N, E^N - \operatorname{car}(dz))$. Then if α_1 is a C^∞ cycle in the same class in $\mathfrak{K}^n(U, V)$ as α, $d\alpha_1$ is in the same class of $\mathfrak{K}^n(V)$ as $d\alpha$. Thus we have

$$(\alpha, dz) = \int_{\alpha_1} dz, \qquad (d\alpha, z) = \int_{d\alpha_1} z.$$

By Stoke's theorem, these two expressions are equal.

(2) Let $j: (A, B) \to (A_1, B_1)$. Let $z \varepsilon Z_n(A_1, B_1)$, and let $j': E^N \to E^N$ be an extension of j. Let j_i be a sequence of C^∞ maps which converge uniformly to j' on every compact set. Then for i sufficiently large, $j_i{}^*z$ is in the same class of $H_n(A, B)$ as j^*z. Choose some such i. Let α be a singular cycle of A modulo B. We put

$$(U_1, V_1) = (E^N - \operatorname{car}(dz), E^N - \operatorname{car}(z)), \qquad (U, V) = (j_i)^{-1}(U_1, V_1).$$

We let (U_2, V_2) be a pair of neighborhoods of (A, B) such that $(U_2, V_2) \subseteq (U, V)$, and such that if $x \varepsilon U$ (or, V) then the whole segment between $j(x)$ and $j_i(x)$ is in U_1 (or, V_1). Let α_2 be a C^∞ cycle in the same class of $\mathfrak{K}^n(U_2, V_2)$ as α; then it follows by homotopy that $j_i\alpha_2$ is in the same class of $\mathfrak{K}^n(U_1, V_1)$ as $j\alpha$. Hence

$$(j\alpha, z) = (j_i\alpha_2, z) = (\alpha_2, j_i{}^*z) = (\alpha_2, j^*z).$$

(3) That $H_0(P)$ and $\mathfrak{k}^n(P)$ are dually paired is clear from the definitions.

§4. The de Rham groups of general pairs. All question as to the nature of the de Rham groups for non-triangulable pairs (S, T) is settled by the following

THEOREM 5. *The groups $H_n(S, T)$ are naturally isomorphic to the Čech cohomology groups (with real coefficients) of the compact pair S, T.*

Proof. Let (S_k, T_k) be a sequence of triangulable pairs such that $(S_k, T_k) \supseteq (S_{k+1}, T_{k+1})$ and $\bigcap_{k=1}^{\infty} (S_k, T_k) = (S, T)$. Then the identity map $i_k:(S_{k+1}, T_{k+1}) \to (S_k, T_k)$ determines a map $i_k{}^*H_l(S_k, T_k) \to H_l(S_{k+1}, T_{k+1})$, so that we have a direct sequence of homology groups. In the same way, the identity map $j_k:(S, T) \to (S_k, T_k)$ determines a map $j_k{}^*: H_l(S_k, T_k) \to H_l(S, T)$. It is clear from the definitions of the groups that each $\alpha \in H_l(S, T)$ is in $j_k{}^*H_l(S_k, T_k)$ for all sufficiently large k. Moreover, $j_k{}^*\beta = 0$ for $\beta \in H_l(S_k, T_k)$ if and only if $i_{k+p}{}^*i_{k+p-1}{}^* \cdots i_k{}^*\beta = 0$ for some sufficiently large p. It follows that $H_l(S, T) =$ direct limit $H_l(S_k, T_k)$, and once this is established, our result follows readily from Theorem X. 3. 1 (Cf. also Theorem X. 12. 1) of Eilenberg-Steenrod [2].

§5. Open manifolds. Suppos that M is a manifold which is not compact but only the union of a countable infinity of compact subsets, and that we consider subsets S, T which are not compact but only closed. Then there are two principal types of de Rham cohomology groups which can be introduced on M:

(a) If we let all forms be forms with compact carriers, we get spaces which can be denoted $F_k{}^c, Z_k{}^c, \cdots, H_k{}^c(M; S, T)$.

(b) If we let all forms be forms with unrestricted carriers, we get spaces of forms which can be denoted $F_k{}^u, Z_k{}^u, \cdots, H_k{}^u(M; S, T)$.

Of course, if S is compact, or if the closure of the complement of T is compact, the groups $H_k{}^u(M; S, T)$ and $H_k{}^c(M; S, T)$ are naturally isomorphic. In either of these two cases we can drop the superscript and write simply $H_k(M; S, T)$ as in §1-4.

The groups $H_k{}^c(M; S, T)$ seem to be the more interesting of the two types of de Rham groups. Part of this interest stems from the following obvious but important

THEOREM 6. *If M is a C^∞ manifold, and (S, T) is a pair of closed subsets of M, then $H_k^c(M; S, T)$ and $H_k^c(M-T; S-T)$ are naturally isomorphic.*

To prove this theorem, we have only to examine the definitions of the two groups. As is well known, Theorem 6 is essentially involved in the proof of separation theorems by means of homology theory.

The groups H_k^c and H_k^u are related to the two types of cohomology groups which we can obtain by taking direct and inverse limits over the directed family of compact subsets of M. Indeed, let C_n be a sequence of compact subsets of M such that interior $(C_{n+1}) \supseteq C_n$ and such that $M = \bigcup_{i=1}^{\infty} C_n$. Let D_n be the complement of interior (C_n). Let $S_n^u = C_nS$, $T_n^u = C_nT$. Let $S_n^c = SD_n$, $T_n^c = TD_n$. Then we have identity maps

[*] $$i_n: (S_n^u, T_n^u) \to (S_{n+1}^u, T_{n+1}^u),$$

[**] $$j_n: (S_{n+1}^c, T_{n+1}^c) \to (S_n^c, T_n^c).$$

These maps determine homomorphisms

$$i_n^*: H_k(M; S_{n+1}^u, T_{n+1}^u) \to H_k(M; S_n^u, T_n^u),$$

$$j_n^*: H_k(M; S_n^c, T_n^c) \to H_k(M; S_{n+1}^c, T_{n+1}^c).$$

Thus, the groups $H_k(M; S_n^u, T_n^u)$ form an inverse sequence, and the groups $H_k(M; S_n^c, T_n^c)$ form a direct sequence. We have

THEOREM 7c. *$H^c(M; S, T) =$ direct limit $H(M; S_n^c, T_n^c)$; such a general result is not true for the groups H_k^u, but we have the following weaker*

THEOREM 7u. *Let M be triangulated, and let S and T be subsomplexes of M. Then*

$$H_k^u(M; S, T) = \text{inverse limit } H_k(M; S_n^u, T_n^u).$$

Sketch of Proof of Theorem 7c. Let $\bar{H}_k(M; S, T) =$ direct limit $H_k(M; S_n^c, T_n^c)$. The elements of $\bar{H}_k(M; S, T)$ are certain equivalence classes of elements of $\bigcup_{n=1}^{\infty} H_k(M; S_n^c, T_n^c)$. (For the exact definition of the direct limit group, see Eilenberg-Steenrod [2], pp. 220-222.) Let $\zeta \in \bar{H}_k$, and let $\nu \in H_k(M; S_n^c, T_n^c)$ be in the equivalence class ζ. Let z be a closed form of the class ν. Then z is a closed form with compact carrier, and hence z determines an element η of the group $H_k^c(M; S, T)$ such that $z \in \eta$. We put $h\zeta = \eta$. It follows readily from the exact definition of the equivalence

relation determining the class ζ that the map h is a single-valued linear isomorphism of $\bar{H}_k(M; S, T)$ onto $H_k{}^c(M; S, T)$.

A simple example suffices to show that Theorem 7u cannot be stated in as simple a form as Theorem 7c. Indeed, let M be the Euclidean plane. Let A_∞ be the union of the three segments connecting the four points $(\infty, 1)$, $(0, 1)$, $(0, -1)$, and $(\infty, -1)$ in the order indicated. Let A_n be the union of the three segments connecting the four points $(\frac{1}{n}, 1 - \frac{1}{n})$, $(n, 1 - \frac{1}{n})$, $(n, -1 + \frac{1}{n})$, and $(\frac{1}{n}, -1 + \frac{1}{n})$ in the order indicated. Let $S = A_\infty \cup \bigcup_{i=2}^{\infty} A_n$. Then S is a closed subset of the place. Let C_n be the closed square surface with horizontal sides, center at the origin, and side-length $2n + 1$. It is clear that $H_1(S \cap C_n) = 0$, so that

$$\text{inverse limit } H_1(S \cap C_n) = 0.$$

On the other hand, we shall show that $H_1{}^n(M; S)$ is not zero. Let $\theta(P)$ be the angle that the arc from $(1, 0)$ to p makes with the horizontal, and let $r(p)$ be the length of this arc. Let $v(p)$ be a C^∞ vector field in M which has the value $(r^{-1} \sin\theta, -r^{-1}\cos\theta)$ in the neighborhood of S. Then v is closed in the neighborhood of S. Now, if $v = df$ in the neighborhood U of S, then $\int_C v = 0$ for every closed arc in U. On the other hand, it is clear that every neighborhood of S contains a closed arc C surrounding the origin once in the positive sense, and we have $\int_C v = 2\pi$ along any such arc.

Let us now proceed to the

Proof of Theorem 7u. Let $\bar{H}_k(M; S, T) =$ inverse limit $H_k(M; S_n{}^u, T_n{}^u)$. We define a homomorphism h of $H_k{}^u = H_k{}^u(M; S, T)$ into $\bar{H}_k = \bar{H}_k(M; S, T)$ as follows: let $\alpha \in H_k{}^u$, and let z be a form in the class α. Then $z = 0$ in a neighborhood of T, and $dz = 0$ in a neighborhood of S. Hence $z \in Z_k(M; S_n{}^u, T_n{}^u)$, so that z belongs to a well-determined class $\alpha_n \in H_k(M; S_n{}^u, T_n{}^u)$. It is easily seen that $i_n{}^*\alpha_{n+1} = \alpha_n$, so that the sequence $\alpha_1, \alpha_2, \alpha_3, \cdots$ determines an element α^* of the inverse limit group $\bar{H}_k(M; S, T)$. We define the linear map h by putting $h\alpha = \alpha^*$. To prove Theorem 7u we have only to show that h is an isomorphism of $H_k{}^u$ onto $\bar{H}_k$. It may be remarked that the fact that h is a mapping onto $\bar{H}_k$ is independent of the triangulability of S. We shall prove that h is a mapping onto first, and then shall prove that $h\alpha = 0$ implies $\alpha = 0$.

Proof that h is onto: Let $\beta_1, \beta_2, \beta_3, \cdots$ be a sequence determining an

element β^* in the limit group $\bar{H}_k$, so that $i_n{}^*\beta_{n+1} = \beta_n$. Let $z_1, z_2, z_3, \cdots$ be a sequence of closed forms such that z_k belongs to the class β_k. We shall show that it is possible to choose z_k' in the same class β_k as z_k in such a way that $z_{k+1}' = z_k'$ near C_k. Once this is done, we have only to put $z = \lim_{k\to\infty} z_k$ and take $\beta \varepsilon H_k{}^u$ to be the class of z. This done, we have $h\beta = \beta^*$, so that h maps $H_k{}^u$ onto $\bar{H}_k$.

We make our central construction inductively. Put $z_1' = z_1$. Suppose that z_k' is defined for $k < n$ in such a way as to ensure (a) $z_k' \varepsilon \beta_k$, $k < n$ and (b) $z_k' = z_{k-1}'$ in a neighborhood of C_{k-1}, $k < n$. Then since $i_{n-1}{}^* z_n$ is also in the class β_{n-1}, there exists forms a and b such that $z_n = z_{n-1}' + da + b$, where $a \equiv 0$ in a neighborhood of $T_{n-1}{}^u$ and $b \equiv 0$ in a neighborhood of $S_{n-1}{}^u$. Define a' and b' in such a way that a' and b' are C^∞ forms on M and so that (i) $a' = 0$ in a neighborhood of C_{n-1}; (ii) $a' = a$ in a neighborhood of $T_n{}^u$; (j) $b' = 0$ in a neighborhood of C_{n-1}; (jj) $b' = b$ in a neighborhood of $S_n{}^u$. This is possible since $a \equiv 0$ in a neighborhood of $C_{n-1} \cap T_{n-1}{}^u$, and $b \equiv 0$ in a neighborhood of $C_{n-1} \cap S_n{}^u = S_{n-1}{}^u$. Now put

$$z_n' = z_{n-1}' + da' + b'.$$

Then $z_n' = z_{n-1}'$ in a neighborhood of C_{n-1}, and also

$$z_n' = z_n + d(a' - a) + (b' - b).$$

Since $a' - a \equiv 0$ in a neighborhood of $T_n{}^u$ and $b' - b \equiv 0$ in a neighborhood of $S_n{}^u$, z_n' and z_n both belong to the class β_n. Thus we have completed the inductive step in the construction of the sequence $z_1', z_2', z_3', \cdots$. Consequently, we have shown that h maps $H_k{}^u$ onto $\bar{H}_k$.

Proof that $h\alpha = 0$ implies $\alpha = 0$. At this point, we must introduce the hypothesis that S is a subcomplex of a triangulation of M. Since the particular sequence C_n of compact sets that we use to exhaust M does not affect the limit-group (cf. Eilenberg-Steenrod [2], pp. 219-220) we can assume, without loss of generality, that C_n is a finite subcomplex of M. Let z be an element of the class α. To say that $h\alpha = 0$ is to say that z belongs to the class zero in each of the groups $H_k(M; S_n{}^u, T_n{}^u)$. Thus, for each n, there exists a form a_n which vanishes in a neighborhood of $T_n{}^u$ such that $z \equiv da_n$ in a neighborhood of $S_n{}^u$. Now, $d(a_{n+1} - a_n) = 0$ in a neighborhood of $S_n{}^u$, so that $a_{n+1} - a_n$ belongs to a certain cohomology class; i. e., $a_{n+1} - a_n$ determines an element of $H_k(M; S_n{}^u, T_n{}^u)$. Our first aim is to show that we can choose the sequence a_n in such a way that $a_{n+1} - a_n$ determines the zero element of $H_{k-1}(M; S_n{}^u, T_n{}^u)$.

Let $A_n^{(1)}$, $n = 1, 2, \cdots$ be the set of all a such that $a \equiv 0$ in a neighborhood of T_n^u and $z \equiv da$ in a neighborhood of S_n^u. Choose $b_1 \varepsilon A_1^{(1)}$. Let $G_n^{(1)} \subseteq H_{k-1}(M; S_1^u, T_1^u)$ be the set of all cohomology classes determined by the elements of $b_1 - A_n^{(1)}$. Then $G_n^{(1)} \supseteq G_{n+1}^{(1)}$, and each G_n is a non-null linear variety. Since S_1^u and T_1^u are finite subcomplexes of M, $H_{k-1}(M; S_1^u, T_1^u)$ is finite dimensional. Hence $\bigcap_{n=2}^{\infty} G_n^{(1)} = G^{(1)}$ is non-null. Let $\alpha_1 \varepsilon G^{(1)}$, and let d_1 be an element of the cohomology class α_1. Put $a_1 = b_1 + d_1$.

Let $A_n^{(2)}$, $n = 2, 3, \cdots$, be the set of all elements $a \varepsilon A_n^{(1)}$ such that $a_1 - a$ belongs to the zero class of $H_k(M; S_1^u, T_1^u)$. It follows from the construction of a_1 that each $A_n^{(2)}$ is non-null. Let $b_2 \varepsilon A_2^{(2)}$, and let $G_n^{(2)} \subseteq H_{k-1}(M; S_2^u, T_2^u)$ be the set of all cohomology classes determined by the elements of $b_2 - A_n^{(2)}$. Then $\bigcap_{n=3}^{\infty} G_n^{(2)} = G^{(2)} \neq \emptyset$. Let $\alpha_2 \varepsilon G^{(2)}$, and let d_2 be an element of the class α_2. Put $a_2 = b_2 + d_2$. Then, continuing inductively, define $a_3, a_4, \cdots$ in such a way that $a_{n+1} - a_n$ always belongs to the zero class of $H_{k-1}(M; S_n^u, T_n^u)$.

Next we will construct a sequence of elements $a_n' \varepsilon A_n^{(1)}$ such that $a_n' = a_{n+1}'$ in a neighborhood of C_n. Once this is done, we have only to take $a = \lim_{n\to\infty} a_n'$ in order to have $a \equiv 0$ in a neighborhood of T and $z \equiv da$ in a neighborhood of S. However, the existence of such an a means precisely that z belongs to the zero class of $H_k^u(M; S, T)$, i. e., that $\alpha = 0$. Thus, all that remains is the construction of the sequence a_n'.

We make the construction inductively. Put $a_1' = a_1$. Suppose that a_m' has been defined for $m < n$ in such a way as to ensure that (a) $a_m' \varepsilon A_m^{(1)}$; (b) $a_m' - a_m$ belongs to the zero class of $H_{k-1}(M; S_m^u, T_m^u)$; (c) $a_m' - a_{m-1}' \equiv 0$ in some neighborhood of C_{m-1}, for $m < n$. Then a_n can be written in the form $a_n = a_{n-1}' + db + c$, where $b \equiv 0$ in a neighborhood of T_{n-1}^u, and $c \equiv 0$ in a neighborhood of S_{n-1}^u. Let b' and c' be C^∞ forms on M such that (i) $b' = 0$ in a neighborhood of C_{n-1}; (ii) $b' = b$ in a neighborhood of T_n^u; (j) $c' = 0$ in a neighborhood of C_{n-1}; (jj) $c' = c$ in a neighborhood of S_n^u. This is possible since $b = 0$ in a neighborhood of $C_{n-1} \cap T_n^u = T_{n-1}^u$ and $c = 0$ in a neighborhood of $C_{n-1} \cap S_n^u = S_{n-1}^u$. Put $a_n' = a_{n-1}' + db' + c'$. Then $a_n' = a_n + d(b - b') + (c - c')$. It follows readily that $a_n' \varepsilon A_n^{(1)}$, that $a_n' - a_n$ is in the zero class of $H_{k-1}(M; S_n^u, T_n^u)$, and that $a_n' - a_{n-1}' \equiv 0$ in a neighborhood of C_{n-1}. This concludes our inductive step, and with it, our proof of Theorem 7*u*.

Now if M is triangulated, and S and T are subcomplexes of M, then it

is known that the singular homology group $\mathfrak{K}_c^n(S, T)$ of finite cycles arises as the limit group of the direct sequence of homology groups obtained from the sequence of identity maps i_n of [*]. Moreover, it is known that the singular homology group $\mathfrak{K}_u^n(S, T)$ of locally finite cycles arises as the limit group of the inverse sequence of homology groups obtained from the sequence of identity maps j_n of [**]. Now, in the case in which all terms are finite dimensional vector spaces, the inverse limit of an inverse sequence is dually paired to the direct limit of the direct sequence of dual groups. (Cf. Lefschetz [3], 120. 81, p. 67, and also 6, pp. 74-83, especially 33, p. 83). We have therefore

THEOREM 8c. *Let M be a triangulable C^∞ manifold, and let (S, T) be a pair of subcomplexes of M. Then $H_k^u(M; S, T)$ and $\mathfrak{K}_c^k(S, T)$ are dually paired under the natural pairing defined by the integral of a k-form over a finite k-chain.*

THEOREM 8u. *Let M be a triangulable C^∞ manifold, and let (S, T) be a pair of subcomplexes of M. Then $H_k^c(M; S, T)$ and $\mathfrak{K}_u^k(S, T)$ are dually paired under the natural pairing defined by the integral of a k-form with compact carrier over a locally finite k-chain.*

YALE UNIVERSITY.

BIBLIOGRAPHY.

[1] S. Eilenberg, "Singular homology in differentiable manifolds," *Annals of Mathematics*, vol. 48 (1947), p. 670.

[2] S. Eilenberg and N. Steenrod, *Foundations of Algebraic Topology*, Princeton, 1952.

[3] S. Lefshetz, *Algebaic Topology*, American Mathematical Society Colloquium Publications, vol. 27 (1942).

ASYMPTOTIC INTEGRATIONS OF LINEAR DIFFERENTIAL EQUATIONS.*

By Philip Hartman and Aurel Wintner.

Introduction.

In the linear system of differential equations

$$y' = (J + G(t))y, \tag{i}$$

where y' denotes dy/dt and y is a (column) vector with d components, let J be a d by d matrix of complex numbers, and $G(t)$ a d by d matrix of continuous (possibly complex-valued) functions $g_{jk}(t)$ on the half-line $0 \leqq t < \infty$. Let $\lambda_1, \cdots, \lambda_d$ denote the characteristic numbers of J and $\mu_j = \operatorname{Re} \lambda_j$ the real part of λ_j. Finally, put

$$| G(t) | = \sum_{j=1}^{d} \sum_{k=1}^{d} | g_{jk} |. \tag{ii}$$

Part I of this paper deals with the asymptotic integration of (i) on a logarithmic scale. If

$$| G(t) | \to 0 \text{ as } t \to \infty, \tag{iii}$$

then (i) has d linearly independent solutions $y(t) = y_1(t), \cdots, y_d(t)$ with the property that, if $| y |$ denotes the length of the vector y,

$$\lim_{t \to \infty} t^{-1} \log | y(t) | = \mu, \tag{iv}$$

where $\mu = \mu_m$, $y(t) = y_m(t)$ and $m = 1, \cdots, d$. This was proved by Perron (cf. [8], pp. 158-159) with the lim replaced by lim sup, but his method can be used to supply (iv) as it stands, cf. [7].

In view of known results ([2], [3]) for the case when (i) is equivalent to a second order differential equation, it is natural to ask under what conditions, weaker than (iii), will the assertion concerning (iv) remain true. In this direction, it will be shown that (iii) can be relaxed to

$$\underset{0 \leqq V < \infty}{\text{l. u. b.}} \int_U^{U+V} | G(t) | \, dt/(1 + V) \to 0 \text{ as } U \to \infty. \tag{v}$$

* Received October 21, 1954.

It is clear that (iii) implies (v) and also that (v) holds if $|G(t)|$ is of class $L^p(0,\infty)$ for some $p \geqq 1$. (When $\mu_1 = \cdots = \mu_d$, condition (v) can be relaxed to

$$T^{-1} \int_0^T |G(t)|\, dt \to 0,$$

as $T \to \infty$.)

The fact that (v) implies the statement concerning (iv) is a corollary of (*) in Section 2 below. In contrast to Perron's proof, the proof of (*) will not depend on successive approximations. This leads, among other things, to an extension of (*) to non-linear systems under conditions less severe than those used by Perron in [8] (this extension will be carried out in a forthcoming paper). It also leads to theorems on the asymptotic integration of (i) under conditions different from those in standard theorems; cf. Part III.

Parts II and III will deal with asymptotic formulae for solutions of (i), rather than for the logarithms of their magnitudes. In Part II, there will be deduced (Theorem (**)) a refinement of a theorem obtained by Dunkel in his dissertation [1], written under the direction of Bôcher. Particular cases of this theorem have been rediscovered repeatedly (possibly because the result was published in a periodical which is not readily accessible). On the other hand, as far as we know, the only proof of Dunkel's complete theorem in the literature is that of Dunkel himself. His proof is based on simple ideas but is rather diffcult to read because of complicated computations involved in his successive approximations. It seems to be worthwhile to give a proof which avoids successive approximations. After a suitable change of variables, the main theorem (**) of Part II will be obtained as a corollary of the results of Part I.

If the independent variable x in Dunkel's theorem is replaced by $t = -\log x$, his assertion implies that if $y_0(t) = c \exp \lambda t$, where $c \neq 0$ is a constant vector, is a solution of the system

(vi) $$y' = Jy,$$

if the elementary divisors of J belonging to the characteristic numbers λ_j satisfying $\mu_j = \mu$ ($= \operatorname{Re} \lambda$) are simple, and if

(vii) $$\int^\infty |G(t)|\, dt < \infty,$$

then (i) has a solution $y = y(t)$ satisfying, as $t \to \infty$,

(viii) $$y(t) - y_0(t) = o(e^{\mu t}).$$

More generally, if $y_0 = (c_1 t^k + c_2^{k-1} + \cdots + c_{k+1})\exp\lambda_m t$, where $c_1, \cdots, c_{k+1}$ are constant vectors and $c_1 \neq 0$, is a solution of (vi), if h_* denotes the maximum multiplicity of the elementary divisors of J belonging to the eigenvalues λ_j satisfying $\mu_j = \mu_m$, and if

$$\text{(ix)} \qquad \int^{\infty} t^{h_*-1} \mid G(t) \mid dt < \infty,$$

then (i) has a solution $y = y(t)$ satisfying, as $t \to \infty$,

$$\text{(x)} \qquad y(t) - y_0(t) = o(t^{k-1}e^{\mu t}).$$

It will be shown below that if $h_0 \geqq h_*$ and if condition (ix) is strengthened to

$$\text{(xi)} \qquad \int^{\infty} t^{h_0-1} \mid G(t) \mid dt < \infty, \qquad (h_0 \geqq h_*),$$

then assertion (x) can be improved to

$$\text{(xii)} \qquad y(t) - y_0(t) = o(t^{h_0-h_*+k-1}e^{\mu t}).$$

In particular, if $h_0 \geqq 2h_* - 1$, then (viii) holds. For example, if

$$\text{(xiii)} \qquad \int^{\infty} t^{2(d-1)} \mid G(t) \mid dt < \infty,$$

then to every solution $y = y_0(t)$ of (vi) satisfying (iv), there exists a solution $y = y(t)$ of (i) satisfying (viii).

The assertion (**) in Section 11 refining Dunkel's theorem is stated for the case when J is in its Jordan normal form. This permits a refinement of the assumption (xi) and the assertion (xii). For example, if the d-th order, linear differential equation for the scalar x,

$$\text{(xiv)} \qquad x^{(d)} + f_1(t)x^{(d-1)} + \cdots + f_{d-1}(t)x' + f_d(t)x = 0,$$

is written as a system of first order linear differential equations for the vector $y = (x, x', \cdots, x^{(d-1)})$, then the following fact will follow from (**): If the (possibly complex-valued) coefficients $f_1(t), \cdots, f_d(t)$ of (xiv) are continuous for large t and satisfy

$$\text{(xv)} \qquad \int^{\infty} t^{j-1} \mid f_j(t) \mid dt < \infty \qquad (j = 1, \cdots, d)$$

and if $0 \leqq k \leqq d - 1$, then (xiv) has a solution $x = x(t) = x_k(t)$ satisfying, as $t \to \infty$,

$$\text{(xvi)} \qquad x \sim t^k, x' \sim kt^{k-1}, \cdots, x^{(k)} \sim k!$$

and

$$x^{(k+1)} = o(t^{-1}), \cdots, x^{(d-1)} = o(t^{k-d+1}). \tag{xvii}$$

On the other hand, by the statement of Dunkel's theorem (cf. [1], pp. 368-370), the condition (xv) must be replaced by the stronger requirement that $t^{d-1} \mid f_j(t) \mid$ is of class L for $j = 1, \cdots, d$ and the assertion in (xvii) by the weaker statement that

$$x^{(k+1)} = o(1), \cdots, x^{(d-1)} = o(1) \tag{xviii}$$

as $t \to \infty$. (Of course, when the coefficients $f_j(t)$ are not "close to 0" in the sense of (xv), but are "near" to other constants, then (**) still furnishes an asymptotic integration of (xiv).)

In Section 17 at the end of Part II, Theorem (**) will be used to obtain the following theorem dealing with a system of the form

$$y' = (P(t) + G(t))y, \tag{xix}$$

in which the constant matrix J in (i) is replaced by a continuous periodic matrix $P(t)$, say of period 1, so that $P(t+1) = P(t)$: If $y = y_0(t)$ is a solution of

$$y' = P(t)y \tag{xx}$$

satisfying (iv) and if $G(t)$ is continuous for large t and satisfies (xiii), then (xix) has a solution $y = y(t)$ satisfying (viii) as $t \to \infty$. (In particular, if $y_0 = e^{\lambda t}p(t)$ is a solution of (xx), where $p(t) \not\equiv 0$ is a vector of period 1, then (xiii) implies that (xix) has a solution $y = y(t)$ satisfying (viii), where $\mu = \operatorname{Re} \lambda$.)

Part III will deal with analogues of the result of Part II, when the conditions (vii), (ix) or (x) are replaced, respectively, by

$$\int^{\infty} | G(t) |^{\gamma} dt < \infty, \quad \int^{\infty} t^{\gamma h_* - 1} | G(t) | dt < \infty \text{ or } \int^{\infty} t^{\gamma h_0 - 1} | G(t) | dt < \infty,$$

where γ is some number on the range $1 \leqq \gamma \leqq 2$. The proof of the main results of Part III depend on a modification of the proof of (*) in Part I.

The results obtained generalize the theorem (VII) in [2], p. 575, dealing with a second order linear differential equation

$$x'' - f(t)x = 0, \tag{xxi}$$

where $f(t)$ is real-valued and "nearly" 1 for large t. The theorems to be obtained for the system (i) allow an extension of theorem (VII) of [2] to cases in which $f(t)$ is complex-valued and "near" a complex number λ,

which is not 0 or a negative real number, and to cases in which $|f(t)| \to \infty$ as $t \to \infty$. For example, it is shown that if λ is a complex number which is neither negative nor zero (so that $\operatorname{Re} \lambda^{\frac{1}{2}} \neq 0$) and if $f(t)$ is a complex-valued continuous function for large t satisfying

$$\int^{\infty} |f(t) - \lambda|^{\gamma} \, dt < \infty \text{ for some } \gamma, \qquad 1 \leqq \gamma \leqq 2,$$

then (xxi) has a pair of solutions satisfying, as $t \to \infty$,

$$x \sim \exp \pm \int^{t} \tfrac{1}{2}(\lambda^{\frac{1}{2}} + \lambda^{-\frac{1}{2}} f(u))\, du, \qquad x' \sim \pm \lambda^{\frac{1}{2}} x.$$

It is also shown that if $f(t)$ is a complex-valued continuously differentiable function such that

$$\text{(xxii)} \qquad \operatorname{Re} f^{\frac{1}{2}}(t) \neq 0, \qquad \int^{\infty} |\operatorname{Re} f^{\frac{1}{2}}(t)| \, dt = \infty, \qquad f' = o(|f| \, |\operatorname{Re} f^{\frac{1}{2}}|),$$

then (xxi) has a pair of solutions satisfying, as $t \to \infty$,

$$\text{(xxiii)} \qquad x' \sim \pm f^{\frac{1}{2}} x.$$

If the last condition in (xxii) is replaced by

$$\text{(xxiv)} \qquad \int^{\infty} |f'/f|^{\gamma} \, |\operatorname{Re} f^{\frac{1}{2}}|^{\gamma-1} \, dt < \infty \text{ for some } \gamma, \text{ where } 1 \leqq \gamma \leqq 2,$$

then (xxi) has solutions satisfying (xxiii) and

$$\text{(xxv)} \qquad x \sim f^{-\frac{1}{4}}(t) \exp \pm \int^{t} f^{\frac{1}{2}}(u)\, du,$$

where $f^{-\frac{1}{4}} = (f^{\frac{1}{2}})^{-\frac{1}{2}}$. Somewhat different asymptotic formulae follow if the three conditions of (xxii) are retained and (xxiv) is replaced by

$$\text{(xxvi)} \qquad \int^{\infty} |d(f'/f^{\frac{3}{2}})| < \infty.$$

In this case, (xxi) has a pair of solutions satisfying (xxiii) and

$$\text{(xxvii)} \qquad x \sim f^{-\frac{1}{4}}(t) \exp \pm \int^{t} f^{\frac{1}{2}}(1 + f'^{2}/16 f^{3})^{\frac{1}{2}} \, du.$$

While the assertion concerning (xxiv) has no analogue in the elliptic case (say, when $f(t)$ is negative), the assertion concerning (xxvi) does: Let $f(t)$ be a continuously differentiable function for large t satisfying

(xxviii) $\qquad f(t) \neq 0$ and $\exp \pm i \int^{t} f^{\frac{1}{2}}(1 + f'^2/16f^3)^{\frac{1}{2}}\, du = O(1),$

(xxvi) and

(xxix) $$\lim_{t\to\infty} (1 + f'^2/16f^3) \neq 0.$$

Then the differential equation

(xxi bis) $$x'' + f(t)x = 0$$

has a pair of solutions satisfying, as $t \to \infty$,

$$x \sim f^{-\frac{1}{4}}(t) \exp \pm i \int^{t} f^{\frac{1}{2}}(1 + f'^2/16f^3)^{\frac{1}{2}}\, du, \qquad x' \sim \text{const.}\, f^{\frac{1}{2}}x,$$

where the const. depends on the value of the limit (xxix).

For corresponding results under different conditions on f, cf. [10].

Part I. The logarithmic scale.

1. Notation. Without loss of generality, it can be supposed that the constant matrix J is in its Jordan normal form; so that J consists of a number of "blocks," say g "blocks," $J(1), \cdots, J(g)$, on its diagonal, where $J(j)$ is an $h(j)$ by $h(j)$ matrix with a certain number $\lambda = \lambda(j)$ on its diagonal and, if $h(j) > 1$, the number 1 on its subdiagonal, where $h(1) + \cdots + h(g) = d$; the numbers $\lambda(1), \cdots, \lambda(g)$ need not be distinct.

The system (vi) reduces to

(1_{j1}) $$y^{j1\prime} = \lambda y^{j1},$$

(1_{jk}) $$y^{jk\prime} = \lambda y^{jk} + y^{j\,k-1}, \qquad k = 2, \cdots, h(j),$$

where $\lambda = \lambda(j)$; $j = 1, \cdots, g$; $h(1) + \cdots + h(g) = d$; $y^m = y^{jk}$ if $m = h(1) + \cdots + h(j-1) + k$ for $k = 1, \cdots, h(j)$. The equations (1_{jk}), $k > 1$, are missing if $h(j) = 1$.

Similarly, (i) can be written as

(2_{j1}) $$y^{j1\prime} = \lambda y^{j1} + g_{j1\,\alpha\beta}y^{\alpha\beta},$$

(2_{jk}) $$y^{jk\prime} = \lambda y^{jk} + y^{j\,k-1} + g_{jk\,\alpha\beta}y^{\alpha\beta}, \qquad k = 2, \cdots, h,$$

where $\lambda = \lambda(j)$, $h = h(j)$; $j = 1, \cdots, g$; the element $g_{m\gamma}(t)$ of the matrix $G(t)$ is written as $g_{m\gamma} = g_{jk\,\alpha\beta}$ if $m = h(1) + \cdots + h(j-1) + k$, $\gamma = h(1) + \cdots + h(\alpha - 1) + \beta$ for $k = 1, \cdots, h(j)$ and $\beta = 1, \cdots, h(\alpha)$;

finally, the summation convention is used for the indices α, β; so that the last term of (2_{jk}) means

$$g_{jk\,\alpha\beta}y^{\alpha\beta}=\sum_{\alpha=1}^{g}\sum_{\beta=1}^{h(\alpha)}g_{jk\,\alpha\beta}y^{\alpha\beta}.$$

It can be supposed that the enumeration has been chosen so that $\mu(j)=\operatorname{Re}\lambda(j)$ satisfies

(3) $$\mu(1)\leqq\cdots\leqq\mu(g).$$

Let the distinct numbers in the set (3) be denoted by $\mu^1<\mu^2<\cdots<\mu^f$. For a given integer m, where $1\leqq m\leqq f$, an integer j on the range $1\leqq j\leqq g$ will be denoted by p, q or r according as $\mu(j)<\mu^m$, $\mu(j)=\mu^m$ or $\mu(j)>\mu^m$:

(4) $$\mu(j)\lesseqgtr\mu^m \text{ according as } j=p,\ q \text{ or } r.$$

In terms of these notations, put

(5) $$L_m=\sum_q\sum_{k=1}^{h(q)}|\,y^{qk}\,|^2;$$

so that L_m is the sum of the squares of the absolute values of the components y^j of y corresponding to which $\operatorname{Re}\lambda_j=\mu^m$. Thus $|\,y\,|^2=L_1+\cdots+L_f$.

2. The main theorem. The main result of Part I can be stated as follows:

(*) *Let $G(t)$ be continuous on $0\leqq t<\infty$ and let*

(6) $$\underset{0\leqq V<\infty}{\text{l. u. b.}}\int_U^{U+V}|\,G(t)\,|\,dt/(1+V)\to 0 \text{ as } U\to\infty,$$

that is, for every set of indices $(jk\,\alpha\beta)$, let

$$\underset{0\leqq V<\infty}{\text{l. u. b.}}\int_U^{U+V}|\,g_{jk\,\alpha\beta}\,|\,dt/(1+V)\to 0 \text{ as } U\to\infty.$$

Let $1\leqq m\leqq f$. Then there exists a positive number T with the property that to any number $t_0\geqq T$ and to any set of $\sum h(q)$ numbers $y_0{}^{qk}$, not all 0, there belongs a unique set of $\sum h(r)$ numbers $y_0{}^{rk}$ such that the solution $y=y(t)$ of (2), determined by the initial conditions

(7_1) $y^{pk}(t_0)=0$; (7_2) $y^{qk}(t_0)=y_0{}^{qk}$; (7_3) $y^{rk}(t_0)=y_0{}^{rk}$,

satisfies, as $t\to\infty$,

(8) $$L_j(t)=o(L_m(t)) \text{ if } j\neq m$$

and

$$\log |y(t)| = (\mu^m + o(1))t. \tag{9}$$

It will follow from the proof of (*) that if $0 \leqq \eta < 1$ and if $T = T_\eta$ is sufficiently large, then (7_1) can be replaced by $y^{pk}(t_0) = y_0^{pk}$, where y_0^{pk} are arbitrary numbers satisfying $\Sigma \mid y_0^{pk} \mid \leqq \eta \Sigma \mid y_0^{qk} \mid$.

It is understood that the subset of initial conditions (7_1) or (7_3) is vacuous if $m = 1$ or $m = f$. Both of these sets of initial conditions are vacuous in the case

$$\mu_1 = \cdot \cdot \cdot = \mu_d, \tag{10}$$

where $f = 1$.

(I) *In the case* (10), *condition* (6) *in* (*) *can be relaxed to*

$$T^{-1} \int^{T} | G(t) | \, dt \to 0 \text{ as } T \to \infty, \tag{11}$$

that is, to

$$T^{-1} \int^{T} | g_{jk\,\alpha\beta} | \, dt \to 0 \text{ as } T \to \infty$$

(*for every set of indices* ($jk\,\alpha\beta$)).

Since (*) shows that there are $\Sigma h(q)$ linearly independent solutions of (i) satisfying (9), it is seen that (*) implies the theorem of Perron mentioned in the Introduction.

Assertion (*) contains as a corollary the following theorem of Perron [8], p. 765:

(II) *Let J be a diagonal matrix with diagonal elements $\lambda_1, \cdot \cdot \cdot, \lambda_d$ satisfying $\mu_1 < \cdot \cdot \cdot < \mu_d$, where $\mu_j = \operatorname{Re} \lambda_j$. Let $G(t)$ be a continuous matrix on $0 \leqq t < \infty$ satisfying*

$$G(t) \to 0 \text{ as } t \to \infty. \tag{12}$$

Then for any m, where $1 \leqq m \leqq d$, the system (i) *has a solution $y = y(t) = (y^1(t), \cdot \cdot \cdot, y^d(t))$, the components $y^j(t)$ of which satisfy, as $t \to \infty$,*

$$y^j(t) = o(y^m(t)) \text{ if } j \neq m, \tag{13}$$

$$y^{m\prime}(t)/y^m(t) \to \lambda_m. \tag{14}$$

In order to deduce this from (*), note that (12) implies (6); so that, under the conditions of (II), assertion (*) is applicable to (i). Hence (i) has a solution satisfying (8), (9). Since J is a diagonal matrix and $\mu_1 < \cdot \cdot \cdot < \mu_d$, the sum in (5) reduces to a single term. Hence, the relations

(8) and (13) are equivalent. The fact that J is a diagonal matrix means that the differential equation for y^m in (i) is

$$y^{m\prime} = \lambda_m y^m + \sum_{j=1}^{d} g_{mj} y^j. \tag{15}$$

Hence (14) follows from (12) and (13).

In (II), in order to assure the existence of a solution satisfying (13), (14) for a given m, the condition that J is a diagonal matrix can be relaxed to the assumption that $\mu_j \neq \mu_m$ for all $j \neq m$ (so that there is only one elementary divisor belonging to λ_k with $\operatorname{Re}\lambda_k = \mu_m$ and this elementary divisor is simple).

An easy example shows that (II) has no simple analogue if $\mu_1 = \cdots = \mu_d$. In fact, if $d = 2$, $\lambda_1 = \lambda_2 = 0$ and $g_{12} = g_{22} = 0$, then (2) becomes

$$y^{1\prime} = g_{11} y^1, \qquad y^{2\prime} = g_{21} y^1.$$

The solutions of this system are

$$y^1 = c_1 \exp \int^t g_{11} ds, \qquad y^2 = c_1 \int^t g_{21} (\exp \int^s g_{11} du) ds + c_2.$$

It is clear that g_{11} and g_{21} can be chosen so as to satisfy $g_{jk} \to 0$ as $t \to \infty$ but to leave quite arbitrary the asymptotic behavior of the ratio y^2/y^1 (for a solution in which $c_1 \neq 0$).

3. Riccati equations. The proof of (*) will be similar to the proof of a particular case of it given in [2]. It will depend on the use of Riccati differential equations as "majorants." (For applications of Riccati equations as "majorants" for certain non-linear differential equations, cf. [5], pp. 353-355.)

LEMMA 1. *Let $f(t)$ be a continuous real-valued function on $0 \leqq t < \infty$ satisfying*

$$\operatorname*{l.u.b.}_{0<S<\infty} \left| \int_T^{T+S} f(t) dt / (1+S) \right| \to 0 \text{ as } T \to \infty, \tag{16}$$

and let $c \neq 0$ be a real number. Then, if $r = r(t)$ is a real-valued solution of

$$r' = cr(1-r) + f(t) \tag{17}$$

for large t,

$$r(\infty) = \lim_{t\to\infty} r(t) \text{ exists and is 0 or 1.} \tag{18}$$

Furthermore, (17) *has, for large* t, *solutions* $r(t)$ *satisfying* $r(\infty)=0$ *and solutions* $r(t)$ *satisfying* $r(\infty)=1$.

This theorem is contained in Theorems (I), p. 560 and (II), p. 564 and in their applications on pp. 570-571 in [2]. The proofs given there imply the following fact:

LEMMA 2. *Let* $c>0$ *and let* $f(t)$ *satisfy the assumption of Lemma* 1. *Then there belongs to every* ϵ, $0<\epsilon<1$, *a* $T_\epsilon=T(\epsilon,f)$ *with the properties that if* $r=r(t)$ *is solution of* (17) *on some* t-*interval* $[t_0,t^0]$, $t_0\geqq T_\epsilon$, *and satisfies*

$$r(t)\geqq 2\epsilon \tag{19}$$

for $t=t_0$, *then* $r(t)$ *can be continued over* $t_0\leqq t<\infty$ *and satisfies*

$$r(t)>\epsilon \tag{20}$$

for all $t\geqq t_0$ (*in particular,* $r(\infty)=1$).

These lemmas have the following analogues in which the differential equation (17) is replaced by a differential inequality:

LEMMA 1 bis. *Let* c *and* $f(t)$ *satisfy the conditions of Lemma* 2 *and, for large* t, *let* $v=v(t)$ *be a continuously differentiable function satisfying*

$$v'\geqq cv(1-v)+f(t). \tag{21}$$

Then either

$$\infty\geqq\liminf_{t\to\infty} v(t)\geqq 1 \tag{22}$$

or

$$-\infty\leqq\limsup_{t\to\infty} v(t)\leqq 0. \tag{23}$$

The analogue of Lemma 2 is

LEMMA 2 bis. *Let* c, $f(t)$ *and* $v(t)$ *satisfy the assumptions of Lemma* 1 bis *and let* ϵ, T_ϵ *be the same as in Lemma* 2. *If, in addition,*

$$v(t)\geqq 2\epsilon \tag{24}$$

for some $t=t_0\geqq T_\epsilon$, *then*

$$v(t)>\epsilon \tag{25}$$

for all $t\geqq t_0$ (*and, therefore,* (22) *holds*).

Lemmas 1 bis and 2 bis follow from Lemma 2 and the fact that if $r(t)$ is a solution of (17) on some t-interval $[t_0,t^0]$ and if $v(t)\geqq r(t)$ at

$t = t_0$, then $v(t) \geqq r(t)$ for $t_0 \leqq t \leqq t^0$. Thus, if (23) fails to hold, then $v(t) \geqq 2\epsilon > 0$ for arbitrarily large $t = t_0$. Hence, if $r(t)$ is determined by the initial condition $r(t_0) = 2\epsilon$, then $r(t)$ can be defined for $t_0 \leqq t < \infty$, (20) is satisfied and $r(\infty) = 1$, while $v(t) \geqq r(t)$, and so (22) holds.

4. Proof of (*). Preliminaries. In the proof of (*), it can be supposed that $f > 1$. For the proof in this case will show that the case $f = 1$ (that is, the case (10) in (I)) is quite simple; cf. the deduction of (41) from (40) below.

Let a be a fixed number on the range $0 < a < 1$, so small that

(26) $$c = c_m = 2(\mu^m - \mu^{m-1} - 2a) > 0 \text{ for } m = 2, \cdots, f.$$

Let $|G(t)|$ denote the scalar function defined by

(27) $$|G(t)| = \sum_{j=1}^{d} \sum_{k=1}^{d} |g_{jk}(t)| = \sum_{j=1}^{g} \sum_{k=1}^{h(j)} \sum_{\alpha=1}^{g} \sum_{\beta=1}^{h(\alpha)} |g_{jk\,\alpha\beta}(t)|;$$

so that (6) holds as a scalar relation if $|G(t)|$ is interpreted to be the function (27).

According as $k = 1$ or $k > 1$, (2_{jk}) shows that, for any solution $y = y(t)$ of (2), the absolute value of

(28) $$(|y^{jk}|^2)' - 2\mu(j)|y^{jk}|^2$$

is majorized by $|G(t)|\cdot|y(t)|^2$ or by $2|y^{jk}y^{j\,k-1}| + |G(t)|\cdot|y|^2$. Since $2|bc| \leqq ab^2 + a^{-1}c^2$ for any pair of numbers b and c, it follows that $2|y^{jk}y^{j\,k-1}| \leqq a|y^{jk}|^2 + a^{-1}|y^{j\,k-1}|^2$. Hence, if the resulting inequality for the modulus of (28) is multiplied by a^{2k} and added for $j = q$, $k = 1, \cdots, h(q)$, it is seen that

(29) $$|L_{ma}' - 2\mu^m L_{ma}| \leqq 2aL_{ma} + da^{-2d}|G(t)|(L_{1a} + \cdots + L_{fa}),$$

where

(30) $$L_{ma} = \sum_{q} \sum_{k=1}^{h(q)} a^{2k}|y^{qk}|^2.$$

Thus (5) and $0 < a < 1$ imply that

(31) $$L_{ma} \leqq L_m \leqq a^{-2d}L_{ma}.$$

For $1 \leqq m < f$, put

(32) $$M = M_m = \sum_{j=1}^{m-1} L_{ja} \text{ and } N = N_m = \sum_{j=m}^{f} L_{ja}.$$

Then (29) shows that

(33_m) $$M' \leqq 2(\mu^{m-1} + a)M + d^2a^{-2d}|G(t)|(M + N),$$

(34_m) $$N' \geqq 2(\mu^m - a)N - d^2a^{-2d}|G(t)|(M + N).$$

If the solution $y=y(t)$ under consideration is not identically 0, so that $M+N\geqq a^{2d}\,|\,y\,|^2>0$ for all t, define $v=v_m(t)$ by

$$v=N/(N+M). \tag{35}$$

Clearly,

$$0\leqq v\leqq 1. \tag{36}$$

The relations $v'=(MN'-M'N)/(M+N)^2$ and $v(1-v)=MN/(M+N)^2$ and the inequalities (33), (34) give

$$v'\geqq c_m v(1-v)-d^2a^{-2d}\,|\,G(t)\,|, \tag{37}$$

where c_m is defined as in (26).

In view of (12) and (26), the function $f(t)=-d^2a^{-2d}\,|\,G(t)\,|$ and the constant $c=c_m$ in the differential inequality (37) satisfy the conditions of Lemmas 1 bis and 2 bis in Section 3.

5. The case $m=f$. The proof for the case $m=f$ can be completed at once. For, in this case, the set of conditions (7_3) belonging to y^{rk} is vacuous. Let $y=y(t)$ be the solution of (2) determined by (7_1)-(7_2). Then $y(t)\not\equiv 0$, since not all of the numbers $y_0{}^{qk}$ are 0. Hence $v(t)$ is defined and is a continuously differentiable function on $0\leqq t<\infty$ satisfying the differential inequality (37). Since (7) implies $M(t_0)=0$ and $N(t_0)>0$, it follows that $v(t_0)=1$, by (35). Thus Lemma 1 bis shows that if t_0 is sufficiently large, then $\liminf_{t\to\infty} v(t)=1$. From (36),

$$v(t)\to 1 \text{ as } t\to\infty. \tag{38}$$

The definitions (32), (35) and $m=f$ show, therefore, that, as $t\to\infty$,

$$L_{ja}(t)=o(L_{ma}(t)) \text{ if } j\neq m. \tag{39}$$

In view of (31), this proves assertion (8). By (29) and (39),

$$|\,L_{ma}'-2\mu^m L_{ma}\,|\leqq\{2a+da^{-2d}(1+o(1))\,|\,G(t)\,|\}L_{ma}, \tag{40}$$

since $m=f$. Thus (11) implies that, as $t\to\infty$,

$$|\,t^{-1}\log L_{ma}-2\mu^m\,|\leqq 2a+da^{-2d}o(1)$$

or, by (31),

$$|\,t^{-1}\log L_m-2\mu^m\,|\leqq 2a+da^{-2d}o(1)-t^{-1}\log a^{2d}.$$

Consequently,

$$\limsup_{t\to\infty}\,|\,t^{-1}\log L_m-2\mu^m\,|\leqq 2a. \tag{41}$$

Since $a > 0$ can be chosen arbitrarily small, (9) follows from (8) and (41). This proves the case $m = f$ of (*).

6. The case $m < f$. If $m < f$, introduce, in addition to (35), the auxiliary function $w = v_{m+1}(t)$ defined by

$$w = N_{m+1}/(N_{m+1} + M_{m+1}). \tag{42}$$

Then (42) satisfies

$$0 \leqq w \leqq 1 \tag{43}$$

and the case of (37) in which m is replaced by $m + 1$, that is,

$$w' \geqq c_{m+1} w(1 - w) - d^2 a^{-2d} \mid G(t) \mid. \tag{44}$$

In view of (12) and (26), the function $f(t) = - d^2 a^{-2d} \mid G(t) \mid$ and the constants $c = c_m, c_{m+1}$ in (37) and (44) satisfy the conditions of Lemmas 1 bis and 2 bis in Section 3. Choose ϵ to be $\frac{1}{2}$ and 1 in those assertions and let T be chosen so as to be applicable in the sense of Lemma 2 bis to the differential inequalities (37) and (44). Put $T = \max(T_{\frac{1}{2}}, T_1)$. It will be shown that T has the properties asserted in (*).

The case $\epsilon = 1$ of Lemma 2 bis shows that if $t_0 \geqq T$ and if

$$v(t_0) = 1, \tag{45}$$

then

$$v(t) \geqq \tfrac{1}{2} \tag{46}$$

holds for $t_0 \leqq t < \infty$. Also, the case $\epsilon = \frac{1}{2}$ of Lemma 2 bis shows that if

$$w(t_1) = 0 \text{ for some } t_1 > t_0, \tag{47}$$

then

$$w(t) \leqq \tfrac{1}{2} \tag{48}$$

for $t_0 \leqq t \leqq t_1$, since $w(t) > \frac{1}{2}$ for some t, where $t_0 \leqq t < t_1$, would imply that (47) cannot hold (in fact, that $w(t_1) \geqq \frac{1}{4} > 0$).

7. The solution $y_n(t)$. The existence of the initial conditions (7_3) (belonging to a given $t_0 \geqq T$ and to (7_2)) with the property that (7_1)-(7_3) assure (8) and (9) will be proved by a limit process. If t_0 ($\geqq T$) and if not all of the constants in (7_2) are 0, it will be shown that, corresponding to any $n > t_0$, there exists a (unique) set of $\Sigma\, h(r)$ numbers y_0^{rk} (depending on n) such that the solution $y = y_n(t)$ of (2) determined by (7) satisfies

$$y^{rk}(n) = 0 \text{ for all } r \text{ and for } k = 1, \cdots, h(r). \tag{49}$$

In order to see this, note that, if $y = y(t)$ is a solution of (2) determined by initial conditions of the type

$$(50) \qquad y^{jk}(t_0) = 0 \text{ for } j = p, q$$

(and not all $y^{rk}(t_0)$ are 0), then the corresponding function $w(t)$ satisfies $w(t_0) = 1$. Consequently, $w(t) \geqq \frac{1}{2} > 0$ for $t_0 \leqq t < \infty$, in particular for $t = n$. But $w(n) > 0$, that is, $N_{m+1}(n) > 0$, implies that (49) cannot hold. In other words, the $\Sigma\, h(r)$-dimensional manifold of solutions of (2) determined by (50) contains $\Sigma\, h(r)$ solution vectors such that the corresponding $\Sigma\, h(r)$-dimensional vectors with components $y^{rk}(t)$ are linearly independent for $t = n (> t_0)$. Thus, if $y^{rk}(n)$ are any $\Sigma\, h(r)$ numbers, there exists a unique set of $\Sigma\, h(r)$ numbers $y_0{}^{rk}$ with the property that the initial conditions (50) and (7_3) determine a solution such that the values of its components y^{rk} at $t = n$ are the preassigned numbers $y^{rk}(n)$.

Consequently, if $y = y^*(t)$ is the solution of (2) determined by

$$y^{jk}(t_0) = 0 \text{ for } j = p, r \text{ and } y^{qk}(t_0) = y_0{}^{qk},$$

then there is a unique set of initial conditions (7_3) such that if $y = y_*(t)$ is the solution determined by (7_3) and (50), then the components y^{rk} of $y_*(t)$ at $t = n$ assume the same values as the components $-y^{rk}$ of $-y^*(t)$ at $t = n$. Hence, $y = y_*(t) + y^*(t)$ satisfies (7) and (49). This is the solution $y = y_n(t)$, the existence of which was to be proved.

8. Completion of the proof of (*): Existence. Let $v = v^n(t)$ and $w = w^n(t)$, when the latter is defined, denote the auxiliary functions (36), (42) belonging to the solution $y = y_n(t)$. Since $y = y_n(t)$ is determined by initial conditions of the type (7), (7_1) shows that $v = v^n$ satisfies (45), hence (46) for $t_0 \leqq t < \infty$. Since $y = y_n(t)$ satisfies (49), it follows that $w = w^n$ satisfies (47) for $t_1 = n\ (> t_0)$, hence (48) for $t_0 \leqq t \leqq n$.

The inequality $w^n(t_0) \leqq \frac{1}{2}$ and the fact that $L^n(t_0) = \sum_q \sum_k a^{2k} \mid y_0{}^{qk} \mid^2$ is independent of n show, by (39), that the numbers $N^n{}_{m+1\ a}(t_0)$ are bounded for $n > t_0$. In view of (7), this means that the numbers $\mid y_n(t_0) \mid$ are bounded for $n > t_0$. Consequently, there exists a subsequence of the integers $n\ (> t_0)$ such that, if n tends to ∞ through this subsequence, then $\lim y_n(t_0) = y_\infty(t_0)$ exists. In view of the locally continuous dependence of solutions of (2) on initial conditions, this implies that

$$(51) \qquad \lim y_n(t) = y_\infty(t)$$

exists uniformly on every finite t-interval, as n tends to ∞ through this subsequence of the integers n, and is a solution of (2).

In what follows, n will denote an integer in a subsequence of the integers ($> t_0$) of the type just described.

Clearly, $y = y_\infty(t)$ belongs to initial conditions of the type (7). Hence the corresponding function $v = v^\infty(t)$ satisfies (45) and, therefore, (46) for $t_0 \leqq t < \infty$. It follows from (37), (46) and from Lemma 1 bis that (38) holds for $v = v^\infty(t)$. It is clear from (51) that $w^n(t) \to w^\infty(t)$, as $n \to \infty$, holds uniformly on every finite t-interval. Since $w = w^n(t)$ satisfies (48) for $t_0 \leqq t \leqq t_1$ if $n > t_1$, the function $w = w^\infty(t)$ satisfies (48) for $t_0 \leqq t < \infty$. Consequently (43), (44) and Lemma 1 bis show that

$$(52) \qquad w(t) \to 0 \text{ as } t \to \infty$$

holds for $w = w^\infty(t)$.

The definitions of L_{ma}, M_m, N_m, v and w and the relations (38) and (52) imply (39). The assertions (8), (9) of (*) can be deduced from (39), as in the case $m = f$ treated in Section 5 above.

This completes the proof of the existence of a number T and of the numbers y_0^{rk} having the properties stated.

9. Completion of the proof of (*): Uniqueness. In order to prove the uniqueness of the set of numbers y_0^{rk}, suppose that there are two distinct sets. The difference of the two corresponding solutions determined by (7) is a solution $y = y(t) \not\equiv 0$ satisfying (50). The corresponding function $w = w(t)$ satisfies $w(t_0) = 1$, hence $w(t) \to 1$. Thus $M_{m+1}/N_{m+1} \to$ as $t \to \infty$. From (34_{m+1}),

$$\liminf_{t\to\infty} t^{-1} \log N_{m+1}(t) \geqq 2(\mu^{m+1} - a).$$

The argument leading to (41) and then to (9) shows that

$$\liminf_{t\to\infty} t^{-1} \log |\, y(t)\,|^2 \geqq 2\mu^{m+1}.$$

Since this contradicts the fact that $y = y(t)$ is the difference of two solutions satisfying (9), where $\mu^m < \mu^{m+1}$, the proof of (*) is complete.

10. Variants of (*) and (II). In the proof of (*), just completed, the fact that the eignevalues λ_j of J are constants (independent of t) was used only in order to pass from (39) (or, equivalently, from (8)) to (9). Hence the assertion (8) of (*) remains true if the λ_j are functions of t with the property that there exists a constant $a > 0$ such that

$$(53) \qquad 2(\mu^m - \mu^{m-1} - 2a) \geqq \text{const.} > 0 \quad \text{for} \quad m = 2, \cdots, f.$$

In this case, the number $c = c_m$ of (26) can be replaced by the const. of (53)

in the proof of (39) (and/or (8)). In particular, there results the following analogue of (II):

(II*) *Let* $J = J(t)$ *be a diagonal matrix with diagonal elements* $\lambda_1(t), \cdots, \lambda_d(t)$ *satisfying*

$$\mu_j(t) - \mu_{j-1}(t) \geqq \text{const.} > 0 \text{ for } j = 2, \cdots, d, \tag{54}$$

where $\mu_j(t) = \operatorname{Re} \lambda_j(t)$. *Under the assumption* (6) *on* $G(t)$, *the assertion of* (II) *concerning* (13) *holds. If, in addition,* (12) *is satisfied, then* (14) *is valid in the form*

$$y^{m\prime}(t)/y^m(t) \sim \lambda_m(t) \text{ as } t \to \infty. \tag{55}$$

Under the condition (12), rather than (6), this result is contained in a theorem of Perron [8], p. 763.

For a given m, in order to assure the existence of a solution $y = y(t)$ satisfying (12), the condition that $J = J(t)$ is a diagonal matrix satisfying (54) can be relaxed to the assumption that $J = J(t)$ is in its Jordan normal form for every t and that the eigenvalue $\lambda_m(t)$ satisfies

$$|\mu_m(t) - \mu_j(t)| \geqq \text{const.} > 0 \text{ for } j \neq m \tag{56}$$

for large t. Thus, the (single) elementary divisor belonging to $\lambda_m(t)$ is simple but those belonging to $\lambda_j(t)$, where $j \neq m$, need not be.

For applications in Part II, it will be convenient to have a generalization of (II*) dealing with the case when both the diagonal elements λ_j and the 1's on the subdiagonal of J are replaced by functions of t.

Let the system

$$y' = K(t)y \tag{57}$$

be equivalent to

$$y^{j1\prime} = \lambda y^{j1} \tag{58_{j1}}$$

$$y^{jk\prime} = \lambda y^{jk} + \delta y^{j\,k-1}, \qquad k = 2, \cdots, h(j), \tag{58_{jk}}$$

$j = 1, \cdots, g$; $h(1) + \cdots + h(g) = d$; $\lambda = \lambda(j; t)$ and $\delta = \delta(j; t)$. Thus the diagonal elements of $K(t)$ are $\lambda(j; t)$; its subdiagonal elements are $\delta(j; t)$ or 0; and all other elements of $K(t)$ are 0.

Let $\mu(j; t) = \operatorname{Re} \lambda(j; t)$. Let m be an integer on the range $1 \leqq m \leqq g$ and let c denote a positive constant. Relative to m and c, divide the set of integers $j = 1, \cdots, g$ into three sets, members of which will be denoted by p, q, r, respectively, by the requirements that the integer m is a q; that, for some sufficiently small number a, $0 < a < 1$,

$$\mu(p; t) + a\,|\,\delta p, t)| \leqq \mu(q; t) - a\,|\,\delta(q, t)| - c \tag{59}$$

for all p, q and large t; and that

$$(60) \qquad \mu(r;t) - a\,|\,\delta(r;t)\,| \geqq \mu(q;t) + a\,|\,\delta(q,t)\,| + c$$

for all r, q and large t. Finally, let $L_m(t) = L_m(t;a,c)$ be defined by (5). In terms of this new notation, (*) has the following analogue:

(III) *Let $G(t)$ be continuous on $0 \leqq t < \infty$ and satisfy* (6). *Let the sets of integers $\{p\}$, $\{q\}$, $\{r\}$ and $L_m(t)$ be defined as in the preceding paragraph. Then there exists a positive number T with the property that to any number $t_0 \geqq T$ and to any set of $\Sigma\, h(q)$ numbers y_0^{qk}, not all* 0, *there belongs a unique set of $\Sigma\, h(r)$ numbers y_0^{rk} such that the solution of*

$$(61) \qquad y' = (K(t) + G(t))y$$

determined by the initial conditions (7) *satisfies, as $t \to \infty$,*

$$(62) \qquad y^{jk}(t) = o(L_m^{\frac{1}{2}}(t)) \text{ if } j = p \text{ or } j = r.$$

It is clear that (III) can be extended to the case where $K(t)$ is, for example, a more general triangular matrix. (III) will however suffice for the applications in Part II.

The proof of (III) is very similar to that of (*) and only the beginning of the proof will be indicated. Put

$$L_{ma} = \sum_q \sum_k a^{2k}\,|\,y^{qk}\,|^2; \qquad M = \sum_p \sum_k a^{2k}\,|\,y^{pk}\,|^2; \qquad N = \sum_r \sum_k a^{2k}\,|\,y^{rk}\,|^2.$$

(Here M, N are analogous to M_m, N_{m+1} in Section 4 above). The derivation of (29) shows that

$$(63) \qquad \begin{aligned} L_{ma}' &\leqq 2 \max_q [(\mu(q,t) + a\,|\,\delta(q,t)\,|)]L_{ma} + d\,|\,G(t)\,|\,|\,y(t)\,|^2, \\ L_{ma}' &\geqq 2 \min_q [(\mu(q,t) - a\,|\,\delta(q,t)\,|)]L_{ma} - d\,|\,G(t)\,|\,|\,y(t)\,|^2. \end{aligned}$$

Similarly,

$$M' \leqq 2 \max_p [(\mu(p,t) + a\,|\,\delta(p,t)\,|)]M + d\,|\,G(t)\,|\,|\,y(t)\,|^2,$$

$$N' \geqq 2 \min_r [(\mu(r,t) - a\,|\,\delta(r,t)\,|)]N - d\,|\,G(t)\,|\,|\,y(t)\,|^2.$$

In view of (59)-(60), the number $2c$ (> 0) can play the part of both c_m and c_{m+1} in the proof of (*). The proof can now be completed along the lines of the proof of (*).

Part II. Dunkel's theorem.

11. The main theorem. Part II is concerned with a theorem of Dunkel [1] and refinements of it. In the notation of Section 2, let

$$h_* = \max_q h(q)\,; \tag{64}$$

so that h_* is the maximum of the multiplicities of the elementary divisors of J belonging to eigenvalues λ_k satisfying $\operatorname{Re}\lambda_k = \mu^m$.

The main theorem to be proved is as follows:

(**) *Let μ denote the number μ^m; h_0 a number satisfying*

$$h_* \leqq h_0\,; \tag{65}$$

q_0 a particular value of q; k_0 an integer satisfying $1 \leqq k_0 \leqq h(q_0)$; and b the number

$$b = h_0 - h(q_0) + k_0, \qquad \text{(so that } k_0 \leqq b \leqq h_0). \tag{66}$$

Let $G(t)$ be continuous on $0 \leqq t < \infty$ and suppose that every element $t^{h_0-1}g_{jk\,\alpha\beta}$ of $t^{h_0-1}G(t)$ is of class $L(1,\infty)$ or, more generally, that

$$\int^{\infty} |\, g_{jk\,\alpha\beta} \,|\, t^{\epsilon(\alpha\beta)-\epsilon(jk)+(\epsilon(j)+\epsilon(\alpha)-1)(h_0-h(q_0))}dt < \infty, \tag{67}$$

where $\epsilon(jk)$ is k or 1 according as $j = q$ or $j \neq q$ and $\epsilon(j)$ is 1 or 0 according as $j = q_0$ or $j \neq q_0$. Then the system (2) has a solution $y = y(t)$ with the following asymptotic properties, as $t \to \infty$: When $q = q_0$,

$$y^{qk}(t) = o(e^{\mu t}t^{k-b}) \text{ if } 1 \leqq k < k_0, \tag{68$_1$}$$

$$y^{qk}(t) = e^{\lambda(q)t}t^{k-k_0}/(k-k_0)! + o(e^{\mu t}t^{k-b}) \text{ if } k_0 \leqq k \leqq h(q_0)\,; \tag{68$_2$}$$

when $q \neq q_0$,

$$y^{qk}(t) = o(e^{\mu t}t^{k-b}) \text{ if } 1 \leqq k \leqq h(q)\,; \tag{68$_3$}$$

finally, when $j = p$ or $j = r$,

$$y^{jk}(t) = o(e^{\mu t}t^{1-b}) \text{ if } 1 \leqq k \leqq h(j). \tag{68$_4$}$$

The number h_0 is not required to be an integer. Since $\epsilon(jk) = 1$ if $j \neq q$ and $1 \leqq \epsilon(jk) \leqq h(j) \leqq h_*$ if $j = q$, it is readily verified that (67) holds if

$$\int^{\infty} |\, g_{jk\,\alpha\beta} \,|\, t^{h_0-1}dt < \infty, \tag{67 bis}$$

or if the following pair of conditions on the "rows" of $G(t)$ is satisfied:

$$\int^{\infty} |\, g_{jk\,\alpha\beta}(t) \,|\, t^{h_0-k} dt < \infty \text{ if } j = q, \qquad \int^{\infty} |\, g_{jk\,\alpha\beta}(t) \,|\, t^{h_0-1} dt < \infty \text{ if } j \neq q$$

or if the following pair of conditions on the "columns" of $G(t)$ holds:

$$\int^{\infty} |\, g_{jk\,\alpha\beta} \,|\, t^{h_0-h(\alpha)+\beta-1} dt < \infty \text{ if } \alpha = q, \qquad \int^{\infty} |\, g_{jk\,\alpha\beta} \,|\, t^{h_0-1} dt < \infty \text{ if } \alpha \neq q.$$

After a change of variables, the case $h_0 = h_*$ of (**) is essentially Dunkel's theorem, with certain refinements. In Dunkel's theorem, assumption (67) is strengthened to (67 bis); the estimates (68_1), (68_4) and the cases $k < b$ $(= h_* - h(q_0) + k_0)$ of (68_3) are replaced by the weaker appraisal $y^{jk}(t) = o(e^{\mu t})$, as $t \to \infty$, for the values of j, k indicated; finally, (68_2) is replaced by $y^{qk}(t) \sim e^{\lambda(q)t} t^{k-k_0}/(k-k_0)\,!$, as $t \to \infty$, when $q = q_0$ and $k \geqq k_0$.

It will follow from the proof of (**) that, if t_0 is sufficiently large, a solution $y = y(t)$ satisfying (18) can be chosen so as to satisfy the partial set of initial conditions

$$y^{jk}(t_0) = 0 \tag{69}$$

for

$$j = p;\ j = q_0 \text{ and } k < k_0;\ j = q \neq q_0 \text{ and } k < b. \tag{70}$$

In addition to (69)-(70), one can require that $y^{q_0k}(t_0) = y_0^{q_0k_0} t^{k-k_0}/(k-k_0)\,!$ for $k_0 \leqq k < b$, in which case ($y_0^{q_0k_0}$ and) $y(t)$ is unique.

For the proof of (**) and for other applications, some transformations of (2) under certain changes of variables will be calculated. Before carrying out the computations involved, the change of variables to be employed will be motivated by the following remarks:

Suppose that the matrix J, which, in general, has g $(\geqq 1)$ "blocks" $J(1), \cdots, J(g)$ on its principal diagonal, consists of only one block $J(1)$. Without loss of generality, it can be supposed that the corresponding eigenvalue $\lambda(1)$ is 0. An obvious approach to theorems of type (**) is to attempt to use the variation of constants $y = e^{tJ}z$, which transforms (2) into $z' = e^{-tJ}G(t)e^{tJ}z$. But an element of the matrix $e^{-tJ}G(t)e^{tJ}$ is a linear combination of elements of $G(t)$ with coefficients which are polynomials in t, polynomials of degree n satisfying $0 \leqq n \leqq 2(h(1)-1)$. The fact that a factor as large as $t^{2(h(1)-1)}$ occurs is inconvenient. (Of course, when J consists of more than one block, even factors of the type e^{ct}, $c > 0$, might occur.)

If $J = J(1)$, then e^{tJ} has the factorization $e^{tJ} = De^{J}D^{-1}$, where D is the

diagonal matrix with diagonal elements $1, t, \cdots, t^{h(1)-1}$ and e^J is a constant matrix. It turns out that a more convenient variation of constants is $y = De^Jz$. This variation of constants, when applied to the case $J = J(1)$ of (1), transforms (1) into

$$z^{11\prime} = 0, \quad tz^{12\prime} = z^{12}, \cdots, tz^{1h\prime} = (1 - h)z^{1h};$$

cf. Section 13 below. If the independent variable t is replaced by a new variable defined by $ds = dt/t$, the last system becomes a system belonging to a constant diagonal matrix with distinct diagonal elements $0, -1, \cdots, 1 - h$. Furthermore, $(De^J)^{-1}G(De^J)$ only involves factors as large as $t^{h(1)-1}$ (instead of the $t^{2(h(1)-1)}$ occurring in $e^{-tJ}Ge^{tJ}$).

A variation of constants of the type $y = De^Jz$ was used in [5], p. 724, for a similar purpose.

12. The transformation $y = D_1v$. The changes of variables to be used below will now be considered in detail. After the change of dependent variables $y \to e^{-\mu t}$, where $\mu = \mu^m$, it can be supposed that $\mu^m = 0$. Thus

$$\mu(j) \gtreqless 0 \text{ according as } j = p, q \text{ or } r; \tag{71}$$

cf. (4). It can then be supposed that

$$\lambda(q) = 0, \tag{72}$$

for otherwise the variable y^{qk} could be replaced by $y^{qk}e^{-\lambda(q)t}$. Under this change of (some of the) dependent variables, $g_{jk\,\alpha\beta}$ acquires factors of absolute value 1 (in fact, the factor $e^{\lambda(j)t}$ or 1 according as j is or is not a q, and the factor $e^{-\lambda(\alpha)t}$ or 1 according as α is or is not a q). Thus any assumption on the "smallness" of $| g_{jk\,\alpha\beta} |$ is not affected by this change of variables.

After these preliminaries, both the independent and dependent variables will be changed. The change of independent variables is given by

$$s = \log t, \text{ that is, } t = e^s \qquad (ds = dt/t). \tag{73}$$

It is assumed that the half-line $0 \leqq t < \infty$ has been replaced by $1 \leqq t < \infty$, which then becomes $0 \leqq s < \infty$. The change of dependent variables will be of the form $y = D_1CD_2z$, where D_1 and D_2 are diagonal matrices in which each diagonal element is a power of t to be prescribed and C is a constant matrix. In order to facilitate the computations, it will be convenient to make the changes of variables in successive steps: $y = D_1v$, $v = Cw$ and $w = D_2z$.

Let b denote a fixed number and, for each integer q, let there be given a number $b(q)$. In terms of the numbers b and $b(q)$, define $y = D_1v$ by

$$y^{qk} = t^{k-b(q)}v^{qk} \text{ and } y^{jk} = t^{1-b}v^{jk} \text{ if } j \neq q. \tag{74}$$

If a dot denotes differentiation with respect to s, then (72), (73) and (74) show that the differential system (2) becomes, when $j = q$,

$$(75)\qquad \begin{aligned} \dot{v}^{q1} &= (b(q) - 1)v^{q1} + g_{q1\ \alpha\beta} y^{\alpha\beta}/t^{-b(q)}, \\ \dot{v}^{qk} &= (b(q) - k)v^{qk} + v^{q\ k-1} + g_{qk\ \alpha\beta} y^{\alpha\beta}/t^{k-b(q)-1}, \qquad k > 1, \end{aligned}$$

and, when $j \neq q$,

$$(76)\qquad \begin{aligned} \dot{v}^{j1} &= (\lambda t - 1 + b)v^{j1} + g_{j1\ \alpha\beta} y^{\alpha\beta}/t^{-b}, \\ \dot{v}^{jk} &= (\lambda t - 1 + b)v^{jk} + tv^{j\ k-1} + g_{jk\ \alpha\beta} y^{\alpha\beta}/t^{-b}, \qquad k > 1. \end{aligned}$$

In (76), $\lambda = \lambda(j)$ and $\operatorname{Re}\lambda \neq 0$.

In the non-principal terms of (75)-(76), the variables $y^{\alpha\beta}$ are considered as expressed in terms of t and $v^{\alpha\beta}$ by virtue of (74) and, in addition, $t = e^s$. Let the non-principal terms of (75)-(76) be denoted by $e_{jk\ \alpha\beta} v^{\alpha\beta}$. Then, by (74) and (75)-(76), when $j = q$,

$$(77)\qquad \begin{aligned} e_{qk\ \alpha\beta} &= g_{qk\ \alpha\beta} t^{\beta-k-b(\alpha)+b(q)+1} \text{ if } \alpha \text{ is a } q, \\ e_{qk\ \alpha\beta} &= g_{qk\ \alpha\beta} t^{1-k-b+b(q)+1} \text{ if } \alpha \text{ is not a } q, \end{aligned}$$

and, when $j \neq q$,

$$(78)\qquad e_{jk\ \alpha\beta} = g_{jk\ \alpha\beta} t^{\beta-b(\alpha)+b} \text{ if } \alpha \text{ is a } q, \qquad e_{jk\ \alpha\beta} = g_{jk\ \alpha\beta} t \text{ if } \alpha \text{ is not a } q.$$

The matrix $\| e_{jk\ \alpha\beta} \|$ will be denoted by $E = E(s)$.

13. The transformation $v = Cw$. The constant matrix C in the variation of constants $v = Cw$ consists of g blocks $C(1), \cdots, C(g)$ on its principal diagonal and has 0 for all its other elements. $C(j)$ is an $h(j)$ by $h(j)$ matrix which is $e^{J(j)}$ or the unit $h(j)$-matrix according as $j = q$ or $j \neq q$, where $J(1), \cdots, J(g)$ are the blocks of J. Thus $v = Cw$ can be represented as

$$(79)\qquad v^{jk} = \sum_{n=1}^{k} w^{jn}/(k-n)! \text{ or } v^{jk} = w^{jk}$$

according as $j = q$ or $j \neq q$. The inverse C^{-1} consists of the g blocks $C^{-1}(j)$ on its principal diagonal, where $C^{-1}(j)$ is $e^{-J(j)}$ or the unit $h(j)$-matrix according as $j = q$ or $j \neq q$.

It is readily verified that, for any scalar c,

$$\begin{bmatrix} c-1 & & & & \\ 1 & c-2 & & & \\ & 1 & \cdot & & \\ & & \cdot & \cdot & \\ & & & \cdot & \cdot \\ & & & 1 & c-h \end{bmatrix} C(j)$$

$$= C(j) \begin{bmatrix} c-1 & & & & \\ & c-2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & c-h \end{bmatrix},$$

where $h = h(j)$ and the matrix elements not indicated are 0. Thus the transformation (79) has the effect of diagonalizing the principal terms of (75). The system (75)-(76) therefore becomes

$$(80) \qquad \dot{w}^{qk} = (b(q) - h)w^{qk} + h_{qk\,\alpha\beta}w^{\alpha\beta}$$

and, if $j \neq q$,

$$(81) \qquad \begin{aligned} \dot{w}^{j1} &= (\lambda t - 1 - b)w^{j1} + h_{j1\,\alpha\beta}w^{\alpha\beta}, \\ \dot{w}^{jk} &= (\lambda t - 1 - b)w^{jk} + tw^{j\,k-1} + h_{jk\,\alpha\beta}w^{\alpha\beta}, \qquad k > 1, \end{aligned}$$

where $H = \| h_{jk\,\alpha\beta} \|$ is given by $H = C^{-1}EC$.

It is readily verified from (79) and the description of C^{-1} that

$$(82) \qquad \begin{aligned} h_{jk\,\alpha\beta} &= e_{jk\,\alpha\beta} \text{ if neither } j \text{ nor } \alpha \text{ is a } q, \\ h_{jk\,\alpha\beta} &= \sum_{\gamma=\beta}^{h(\alpha)} e_{jk\,\alpha\gamma}/(\gamma-\beta)! \text{ if } j \text{ is not, but } \alpha \text{ is, a } q, \\ h_{jk\,\alpha\beta} &= \sum_{n=1}^{k} (-1)^{k-n} e_{jk\,\alpha\beta}/(k-n)! \text{ if } j \text{ is, but } \alpha \text{ is not, a } q, \\ h_{jk\,\alpha\beta} &= \sum_{n=1}^{k} \sum_{\gamma=\beta}^{h(\alpha)} (-1)^{k-n} e_{jn\,\alpha\beta}/(k-n)!(\gamma-\beta)! \text{ if both } j \text{ and } \alpha \text{ are } q\text{'s}. \end{aligned}$$

It can be noted that $h_{jk\,\alpha\beta}$ is a linear combination, with constant coefficients, of the elements $e_{jn\,\alpha\gamma}$, where j and α are fixed and n $(\leqq k)$, γ $(\geqq \beta)$ vary.

14. The transformation $w = D_2 z$. The last change of variables $w = D_2 z$ is given by

$$(83) \qquad w^{jk} = t^c z^{jk} \text{ if } j = q_0 \text{ and } k \neq k_0, \qquad w^{jk} = z^{jk} \text{ otherwise,}$$

where c is a constant and $t = e^s$. This is the identity transformation if $c = 0$. The system (80)-(81) is transformed by (83) into

$$
(84)\qquad \begin{aligned}
\dot z^{q_0k} &= (b(q_0) - c - k)z^{q_0k} + b_{q_0k\ \alpha\beta}z^{\alpha\beta} \text{ if } k \neq k_0,\\
\dot z^{qk} &= (b(q) - k)z^{qk} + b_{qk\ \alpha\beta}z^{\alpha\beta} \text{ if } q \neq q_0 \text{ or if } (qk) = (q_0k_0),
\end{aligned}
$$

and, if $j \neq q$,

$$
(85)\qquad \begin{aligned}
\dot z^{j1} &= (\lambda t - 1 - b)z^{j1} + b_{j1\ \alpha\beta}z^{\alpha\beta},\\
\dot z^{jk} &= (\lambda t - 1 - b)z^{jk} + tz^{j\ k-1} + b_{jk\ \alpha\beta}z^{\alpha\beta} \text{ if } k > 1,
\end{aligned}
$$

where $B = \| b_{jk\ \alpha\beta} \|$ is the matrix $D_2^{-1}HD_2$.

Since (83) is $w = D_2z$, it is easily verified that, if $k \neq k_0$,

$$
(86_1)\qquad \begin{aligned}
b_{q_0k\ \alpha\beta} &= h_{q_0k\ \alpha\beta} \text{ if } \alpha = q_0, \beta \neq k_0,\\
b_{q_0k\ \alpha\beta} &= h_{q_0k\ \alpha\beta}t^{-c} \text{ if } \alpha \neq q_0 \text{ or if } (\alpha\beta) = (q_0k_0);
\end{aligned}
$$

and, if $j \neq q_0$ or if $(jk) = (q_0k_0)$,

$$
(86_2)\qquad \begin{aligned}
b_{jk\ \alpha\beta} &= h_{jk\ \alpha\beta}t^{c} \text{ if } \alpha = q,\ \beta \neq k_0,\\
b_{jk\ \alpha\beta} &= h_{jk\ \alpha\beta} \text{ if } \alpha = q \text{ or if } (\alpha\beta) = (q_0k_0).
\end{aligned}
$$

15. Estimates for B. The proof of (**) now proceeds as follows: Assume the normalizations (71) and (72). Introduce the change of variables (83) and the successive variations of constants (74), (79) and (83). In (84), the numbers $b(q)$ and b will be chosen as follows:

$$
(87)\qquad b(q_0) = k_0;\quad b(q) = b \text{ if } q \neq q_0;\quad b = h_0 - h(q_0) - k_0
$$

(this number b is the same as in (66)). In (83), let

$$
(88)\qquad c = h(q_0) - h_0 \qquad\qquad (\text{so that } c \leqq 0).
$$

It will be verified that

$$
(89)\qquad \int^{\infty} | b_{jk\ \alpha\beta} |\, ds < \infty \text{ for arbitrary } (jk\ \alpha\beta)
$$

and, in addition, that

$$
(90)\qquad \int^{\infty} e^{-cs}\, | b_{jk\ \alpha\beta} |\, ds < \infty \text{ if } (jk) = (q_0k_0), \qquad (e^{-cs} = t^{h_0 - h(q_0)}).
$$

To this end, the matrices E, H and B will be examined in turn. In view of (87) and the relations (77)-(78), it is seen that $e_{q_0k\ \alpha\beta}$ is $g_{q_0k\ \alpha\beta}$ times

$t^{\beta-k+1}$, $t^{\beta-k-b+k_0+1}$ or $t^{1-k-b+k_0+1}$ according as $\alpha=q_0$, $\alpha=q\neq q_0$ or $\alpha\neq q$. In view of the definitions of b in (66) and of $\epsilon(jk)$, $\epsilon(j)$ following (67), it is seen that

$$(91) \qquad |\, e_{jk\ \alpha\beta}\,| = |\, g_{jk\ \alpha\beta}\,|\ t^{\epsilon(\alpha\beta)-\epsilon(jk)+(\epsilon(\alpha)-1)(h_0-h(q_0))+1}$$

if $j=q_0$. If $q\neq q_0$, then $e_{qk\ \alpha\beta}$ is $g_{qk\ \alpha\beta}$ times $t^{\beta-k-k_0+b+1}$, $t^{\beta-k+1}$ or t^{1-k+1} according as $\alpha=q_0$, $\alpha=q\neq q_0$ or $\alpha\neq q$. Thus (91) holds if $j=q\neq q_0$. Finally, if $j\neq q$, then $e_{jk\ \alpha\beta}$ is $g_{jk\ \alpha\beta}$ times $t^{\beta-k_0+b}$, t^{β} or t according as $\alpha=q_0$, $\alpha=q\neq q_0$ or $\alpha\neq q$. In this case, $j\neq q$, the relation (91) also holds.

Since $ds=dt/t$, it follows from (67) and $\epsilon(j)(h_0-h(q_0))\geqq 0$ that

$$(92) \qquad \int^{\infty} |\, e_{jk\ \alpha\beta}\,|\, ds < \infty,$$

and, from $\epsilon(j)(h_0-h(q_0))=h_0-h(q_0)$ where $j=q_0$, that

$$(93) \qquad \int^{\infty} e^{(h_0-h(q_0))s}\,|\, e_{q_0k\ \alpha\beta}\,|\, ds < \infty \qquad (t=e^s).$$

By (82), the relations corresponding to (92), (93) hold if $e_{jk\ \alpha\beta}$ is replaced by $h_{jk\ \alpha\beta}$. Finally, (89) and (90) follow from these relations, (86) and (88), since $t=e^s$.

16. Completion of the proof of (**). Note that $b(q_0)-c=b$, by (87) and (88), so that the set of differential equations (84) can be rewritten as

$$(94) \qquad \dot z^{qk} = b_{qk\ \alpha\beta}z^{\alpha\beta}$$

if $(qk)=(q_0k_0)$, and as

$$(95) \qquad \dot z^{qk} = (b-k)z^{qk} + b_{qk\ \alpha\beta}z^{\alpha\beta}$$

if $(qk)\neq(q_0k_0)$.

Let (q^*k^*) denote either (q_0k_0) or any pair of indices (qk) such that $q\neq q_0$ and $(h(q)\leqq)k=b$. (For example, if h_0 (and, therefore, b) is not an integer, then the only pair (q^*k^*) is (q_0k_0).) From the definition of (q^*k^*), the differential equation for z^{jk} has the form (94) if and only if $(jk)=(q^*k^*)$. Put

$$(96) \qquad L=L(s)=\Sigma\Sigma\,|\, z^{q^*k^*}|^2.$$

Note that $|(\mathrm{Re}\,\lambda(j)\pm a)t-1+b\,|\geqq$ const. >0 for large t if $a\ (>0)$ is sufficiently small. Thus (III) in Section 10 implies that, for a sufficiently

large S and a given set of numbers $z_0^{q^*k^*}$, not all 0, there exists a unique solution $z = z(s)$ of (84)-(85) satisfying the partial set of initial conditions

$$z^{jk}(S) = 0 \text{ if } j = p;\ j = q \text{ and } k < b \text{ but } (jk) \neq (q_0k_0), \tag{97}$$
$$z^{q^*k^*}(S) = z_0^{q^*k^*}$$

and, as $s \to \infty$, the relation

$$z^{jk} = o(L^{\frac{1}{2}}(s)) \text{ if } (jk) \neq (q^*k^*). \tag{98}$$

It follows from (94), (96) and (98) that

$$|\dot{L}| \leqq \text{const.} |B(s)| L. \tag{99}$$

Consequently (89) implies that, as $s \to \infty$,

$$L(s) = O(1) \text{ and } 1/L(s) = O(1). \tag{100}$$

In particular, $z^{jk}(s) = O(1)$ as $s \to \infty$.

Thus, by (89) and (94),

$$\lim_{s \to \infty} z^{q^*k^*}(s) = z^{q^*k^*}(\infty) \text{ exists.} \tag{101}$$

In particular, $L(\infty)$ exists and $L(\infty) \neq 0$, by the second part of (100). It follows from the superposition principle that if S is fixed and sufficiently large, then to any preassigned set of numbers $z^{q^*k^*}(\infty)$, not all 0, there belongs a unique set of numbers $z_0^{q^*k^*}$, not all zero, with the property that the solution satisfying (97) and (98) also satisfies (101).

Let $z^{q^*k^*}(\infty)$ be 1 or 0 according as $(q^*k^*) = (q_0k_0)$ or $(q^*k^*) \neq (q_0k_0)$. Thus, by (97) and (101), the corresponding solution satisfies, as $s \to \infty$,

$$z^{jk} \to 1 \text{ or } z^{jk} = o(1) \tag{102}$$

according as $(jk) = (q_0k_0)$ or $(jk) \neq (q_0k_0)$. In view of (90), (94) and (101), the relation

$$z^{jk}(s) = 1 + \int_s^\infty b_{jk\,\alpha\beta}(u) z^{\alpha\beta}(u)\,du, \tag{103}$$

where $(jk) = (q_0k_0)$, gives the estimate

$$z^{jk} = 1 + o(t^{h(q_0)-h_0}) \text{ if } (jk) = (q_0k_0) \text{ and } t = e^s. \tag{104}$$

By (83) and (88), the corresponding solution $w = w(s)$ of (80)-(81) satisfies, as $s \to \infty$,

$$w^{jk} = o(t^{h(q_0)-h_0}) \text{ if } j = q_0,\ k \neq k_0,$$
$$w^{jk} = 1 + o(t^{h(q_0)-h_0}) \text{ if } j = q_0,\ k = k_0,$$
$$w^{jk} = o(1) \text{ if } j \neq q_0.$$

Thus, by (79), the corresponding vector $v = v(s)$ is

$$v^{jk} = o(t^{h(q_0)-h_0}) \text{ if } j = q_0,\ k < k_0,$$

$$v^{jk} = 1/(k-k_0)! + o(t^{h(q_0)-h_0}) \text{ if } j = q_0,\ k \geqq k_0,$$

$$v^{jk} = o(1) \text{ if } j \neq q_0.$$

Finally, (74) and (87) imply that the corresponding solution $y = y(t)$ of (2) satisfies (68), when the normalization (72) is assumed. This proves (**).

17. An application of (**). This application concerns the asymptotic integration of a linear system of differential equations, in which the coefficient matrix is the sum of a periodic matrix $P(t)$ and of a matrix $F(t)$ which is "small" for large t.

(†) *Let $P(t)$ be a continuous d by d periodic matrix of period* 1,

$$P(t+1) = P(t). \tag{105}$$

Let $F(t)$ be continuous on $0 \leqq t < \infty$ and satisfy

$$\int^{\infty} t^{2(d-1)} |F(t)|\, dt < \infty. \tag{106}$$

Let $x = x_0(t) \not\equiv 0$ be a solution of

$$x' = P(t)x \tag{107}$$

and let $\mu = \lim t^{-1} \log |x_0(t)|$, as $t \to \infty$. Then

$$x' = (P(t) + F(t))x \tag{108}$$

has a solution $x = x(t)$ satisfying

$$x(t) - x_0(t) = o(e^{\mu t}) \text{ as } t \to \infty. \tag{109}$$

Standard theorems state that the system (107) has a fundamental matrix $X = X(t)$ of the form

$$X(t) = Z(t)e^{tJ}, \text{ where } Z(t+1) = Z(t) \tag{110}$$

and J is a constant matrix. This makes it clear that the limit μ exists for any solution $x = x_0(t) \not\equiv 0$ of (107) and $\mu = \operatorname{Re} \lambda$ holds for some characteristic number λ of J.

It will be clear from the proof of (†) that condition (106) can be relaxed and assertion (109) strengthened if the solutions of (107), say the matrix (110), are known. Condition (106), for example, can be weakened by

replacing the $d-1$ in (106) by h_*-1, where h_* is the maximum of the multiplicities of the elementary divisors of J belonging to characteristic numbers λ satisfying $\operatorname{Re}\lambda=\mu$.

The proof of (†) will depend on the fact that the variation of constants

$$x=Z(t)y \tag{111}$$

transforms (107) into $y'=Jy$ and (108) into $y'=(J+G(t))y$, where

$$G(t)=Z^{-1}(t)F(t)Z(t). \tag{112}$$

It is sufficient to verify this transformation of (108), since (107) is the case $F(t)\equiv 0$ of (108). If (111) is substituted into (108), then the resulting differential equation for y is

$$y'=(Z^{-1}(P+F)Z-Z^{-1}Z')y.$$

Differentiation of (110) gives $Z'e^{tJ}+ZJe^{tJ}=PZe^{tJ}$, since $(e^{tJ})'=Je^{tJ}$ and $X(t)$ is a fundamental matrix of (108). Hence $Z'=PZ-ZJ$. If this is substituted into the last formula line, there results the equation $y'=(J+G(t))y$, where $G(t)$ is given by (112).

Since $Z(t)$ is periodic and non-singular, the matrices $Z(t)$ and $Z^{-1}(t)$ are $O(1)$ as $t\rightarrow\infty$. Hence (106) holds if $F(t)$ is replaced by $G(t)$. Thus, according to (**), to any solution $y=y_0(t)\not\equiv 0$ of $y'=Jy$, there corresponds at least one solution $y=y(t)$ of $y'=(J+G)y$ satisfying $y-y_0=o(e^{\mu t})$, as $t\rightarrow\infty$, where $\mu=\lim t^{-1}\log|y_0(t)|$.

The assertion of (†) now follows by choosing $y_0(t)$ to be $Z^{-1}(t)x_0(t)$ and $x(t)$ to be $Z(t)y(t)$.

Part III. Variants and applications.

18. Statement of results. The first portion of Part III concerns asymptotic integrations of (2) under conditions different from those occurring in (**). The first theorem to be proved is as follows:

(i) *Let $\lambda_1,\cdots,\lambda_d$ be the eigenvalues of the coefficient matrix J in* (1) *and let one of these, say $\lambda=\lambda_m$, satisfy*

$$\mu_m\neq\mu_j \text{ for } j\neq m, \qquad (\mu_k=\operatorname{Re}\lambda_k). \tag{113}$$

Let $G(t)$ be of class L^γ for some γ on the range $1\leqq\gamma\leqq 2$, that is, let

$$\int^{\infty}|G(t)|^{\gamma}\,dt<\infty \text{ for some } \gamma, \text{ where } 1\leqq\gamma\leqq 2. \tag{114}$$

Then (2) *possesses a solution* $y = y(t) = (y^1(t), \cdots, y^d(t))$ *the components of which satisfy, as* $t \to \infty$,

$$(115_1) \qquad y^m(t) \sim \exp \int^t (\lambda_m + g_{mm})\, du,$$

$$(115_2) \qquad y^j(t) = o(|\, y^m(t)\,|) \text{ if } j \neq m.$$

In (115_1), $g_{mm} = g_{mm}(t)$ is the m-th diagonal element of $G(t)$. Assumption (113) implies that the (single) elementary divisor of J for which $\operatorname{Re} \lambda(j) = \mu_m$ is simple. Accordingly, the proof of (i) does not depend on the changes of variables discussed in Sections 12-14 above. The proof of (i) will be given in Section 21 below.

(i) is a generalization of Theorem (VII) in [2], p. 575, dealing with a second order equation $x'' + fx = 0$, where $f = f(t)$ is continuous, real-valued, and $f(t) + 1$ is of class L^γ on $0 \leqq t < \infty$.

Assertion (i) remains valid if the eigenvalues λ_j of J are not constants but are continuous functions $\lambda_j = \lambda_j(t)$ of t, subject to

$$(116) \qquad |\, \mu_j(t) - \mu_m(t)\,| \geqq \text{const.} > 0 \text{ if } j \neq m \qquad (\mu_j = \operatorname{Re} \lambda_j)$$

for large t.

In particular, if $J = J(t)$ is a diagonal matrix with diagonal elements $\lambda_j = \lambda_j(t)$ satisfying (116) for every pair of indices j, m $(\neq j)$, then (i) furnishes the asymptotic behavior of a fundamental set of solutions of (2).

There exists an analogue of (i) which involves no assumption on the elementary divisors of J, but imposes more severe conditions on $G(t)$. This analogue does not contain (i).

(ii) *Let* h_* *be defined by* (64); q_0 *a particular value of* q; k_0 *an integer satisfying* $1 \leqq k \leqq h(q_0)$. *Let* h_0 *be a number satisfing* (65) *and let*

$$(117) \qquad b - k \neq 0 \text{ if } 1 \leqq k \leqq h(q) \text{ and } q \neq q_0,$$

where b *is given by* (66). *For some* γ, *where* $1 \leqq \gamma \leqq 2$, *let*

$$(118) \qquad \int^\infty t^{\gamma h_0 - 1}\, |\, G(t)\,|^\gamma \, dt < \infty$$

or, more generally, for every set of indices $(jk\, \alpha\beta)$, *let*

$$(119) \qquad \int^\infty |\, g_{jk\,\alpha\beta}\,|^\gamma\, t^{\gamma\{\epsilon(\alpha\beta) - \epsilon(jk) + (\epsilon(j) + \epsilon(\alpha) - 1)(h_0 - h(q_0))\} + \gamma - 1}\, dt < \infty,$$

where $\epsilon(jk)$ *and* $\epsilon(j)$ *are defined as after* (67). *Then* (2) *has a solution* $y = y(t)$ *with the following asymptotic properties, as* $t \to \infty$: *When* $q = q_0$,

$$(120_1) \qquad y^{qk} = o(e^{\mu t} t^{k-b} \mid \exp \mid) \text{ if } k < k_0,$$

$$(120_2) \qquad y^{qk} = e^{\lambda(q)t} t^{k-k_0} \exp/(k - k_0)! + o(e^{\mu t} t^{k-b} \mid \exp \mid) \text{ if } k \geqq k_0;$$

when $q \neq q_0$,

$$(120_3) \qquad y^{qk} = o(e^{\mu t} t^{k-b} \mid \exp \mid);$$

finally, when $j = p$ *or* $j = r$,

$$(120_4) \qquad y^{jk} = o(e^{\mu t} t^{1-b} \mid \exp \mid),$$

where

$$(121) \quad \exp = \exp\{\int^t \sum_{k=1}^{k_0} \sum_{\beta=k_0}^{h(q_0)} (-1)^{k_0-k} u^{\beta-k} g_{q_0k\ q_0\beta}(u)\,du/(k_0 - k)!(\beta - k_0)!\}.$$

The condition (117) is vacuous if, for example, there is no q distinct from q_0, that is, if $\operatorname{Re} \lambda(j) \neq \operatorname{Re} \lambda(q)$ when $j \neq q$. The condition (117) holds when h_0 (hence, b) is not an integer.

19. The differential inequalities (37), (44). The proof of (i) will depend on a sharpened form of the differential inequalities (37), (44), occurring in the proof of (*), and on a theorem on Riccati differential inequalities. Assertion (ii) will be reduced essentially to (i) by the changes of variables used for similar purposes in Part II.

In order to obtain the desired differential inequalities, note that the expression $\mid G(t) \mid \cdot \mid y(t) \mid^2$ occurring (twice) in the line following (28) can be replaced by $\mid G \mid \cdot \mid y \mid \cdot \mid y^{jk} \mid$. Thus the derivation of (29) gives

$$\mid L_{ma}' - 2\mu^m L_{ma} \mid \leqq 2aL_{ma} + 2 \mid y \mid \cdot \mid G \mid \cdot \sum_q \sum_k a^{2k} \mid y^{qk} \mid.$$

Since $a^{2k} \mid y^{qk} \mid \leqq a^k \mid y^{qk} \mid \leqq L_{ma}^{\frac{1}{2}}$, the last double sum does not exceed $dL_{ma}^{\frac{1}{2}}$, and so

$$(122_m) \qquad \mid L_{ma}' - 2\mu^m L_{ma} \mid \leqq 2aL_{ma} + 2d \mid y \mid \cdot \mid G \mid L_{ma}^{\frac{1}{2}}$$

can replace (29). This leads to the analogues

$$(123_m) \qquad M_m' \leqq 2(\mu^{m-1} + a)M_m + 2d^2 \mid y \mid \cdot \mid G \mid M_m^{\frac{1}{2}},$$

$$(124_{m+1}) \qquad N_{m+1}' \geqq 2(\mu^{m+1} - a)N_{m+1} - 2d^2 \mid y \mid \cdot \mid G \mid N_{m+1}^{\frac{1}{2}}$$

of (33_m) and (34_{m+1}).

If $L_{ma}(t) \neq 0$ for some t-value (hence for all nearby t-values), then (122_m) can be divided by $2L_{ma}^{\frac{1}{2}}$ to give

$$(125_m) \qquad |(L_{ma}^{\frac{1}{2}})' - \mu^m L_{ma}^{\frac{1}{2}}| \leqq aL_{ma}^{\frac{1}{2}} + d\,|\,y\,|\cdot|\,G\,|.$$

Corresponding to the assumptions $M_m(t) \neq 0$ or $N_{m+1}(t) \neq 0$, (123_m), (124_{m+1}) become, respectively,

$$(126_m) \qquad (M_m^{\frac{1}{2}})' \leqq (\mu^{m-1} + a)M_m^{\frac{1}{2}} + d^2\,|\,y\,|\cdot|\,G\,|,$$

$$(127_{m+1}) \qquad (N_{m+1}^{\frac{1}{2}})' \geqq (\mu^{m+1} - a)N_{m+1}^{\frac{1}{2}} - d^2\,|\,y\,|\cdot|\,G\,|.$$

These differential inequalities make it possible to replace the auxiliary functions (35) and (42) of Sections 4 and 6, respectively, by

$$(128) \qquad v(t) = v_m(t) = N_m^{\frac{1}{2}}/(N_m^{\frac{1}{2}} + M_m^{\frac{1}{2}}),$$

$$(129) \qquad w(t) = v_{m+1}(t) = N_{m+1}^{\frac{1}{2}}/(N_{m+1}^{\frac{1}{2}} + M_{m+1}^{\frac{1}{2}}).$$

If the solution $y = y(t)$ of (2) determining L_{ma}, M_m, N_m is not identically 0, then (128) and (129) are defined, continuous, and satisfy

$$(130_1) \qquad 0 \leqq v \leqq 1; \qquad\qquad (130_2) \qquad 0 \leqq w \leqq 1.$$

If $|\,y\,|$ is replaced by its majorant $a^{-d}(M_m^{\frac{1}{2}} + N_m^{\frac{1}{2}})$ in (125)-(127), then the derivation of (37) in Section 4 shows that (128) satisfies

$$(131) \qquad v' \geqq \tfrac{1}{2}c_m v(1 - v) - d^2a^{-d}\,|\,G\,|, \qquad c_m > 0,$$

provided that $N_m \neq 0$ and $M_m \neq 0$. Similarly,

$$(132) \qquad w' \geqq \tfrac{1}{2}c_{m+1} w(1 - w) - d^2a^{-d}\,|\,G\,|, \qquad c_{m+1} > 0,$$

provided that $N_{m+1} \neq 0$ and $M_{m+1} \neq 0$.

The considerations below will deal with solutions $y = y(t)$ ($\not\equiv 0$) satisfying, as $t \to \infty$,

$$(133_1) \qquad v(t) \to 1, \qquad\qquad (133_2) \qquad w(t) \to 0;$$

so that

$$(134) \qquad M_m = o(L_{ma}) \text{ and } N_{m+1} = o(L_{ma}) \text{ as } t \to \infty.$$

Thus, for large t, $L_{ma} \neq 0$, and so $N_m \neq 0$. For large t, $M_m = 0$ if and only if $v = 1$, while $N_{m+1} = 0$ if and only if $w = 0$. Consequently, for large t, (131) and (132) hold except possibly at those t-values at which $v = 1$ and $w = 0$, respectively.

20. A lemma on Riccati inequalities. Assertion (i) will be obtained from (131), (132) and the following theorem on a Riccati differential inequality:

LEMMA 3. *Let $f = f(t)$ be a real-valued, continuous function on $0 \leqq t < \infty$ and let $f(t)$ be of class L^γ for some γ, where $1 \leqq \gamma \leqq 2$. Let $z = z(t)$ be a real-valued continuous function for large t satisfying*

$$(135) \qquad 0 \leqq z \leqq 1$$

and either

$$(136_1) \qquad z \to 1 \qquad \text{or} \qquad (136_2) \qquad z \to 0$$

as $t \to \infty$. In addition, let $z(t)$ have, on the respective open t-sets $\{z(t) \neq 1\}$, $\{z(t) \neq 0\}$, a continuous derivative satisfying a differential inequality of the form

$$(137) \qquad z' \geqq cz(1 - z) + f, \qquad \text{where } c = \text{const.} > 0.$$

Then, corresponding to the alternatives in (136),

$$(138_1) \quad \int^\infty | z - 1 |^2 \, dt < \infty \qquad \text{or} \qquad (138_2) \quad \int^\infty | z |^2 \, dt < \infty.$$

This lemma is an analogue of (III) in [2], pp. 568-569. As in [2], the assertions "$z - 1$ is of class L^2 or z is of class L^2" can be improved to "$z - 1$ is of class L^γ or z is of class L^γ."

In order to prove Lemma 3, consider the case (136_2) (the other case can be treated similarly). If $[U, V]$ is an interval on which $z > 0$, then (137) is valid on this interval. Multiplication by $z > 0$ does not affect the inequality, and so a quadrature leads to

$$(139) \qquad c \int_U^V z^2(1 - z) dt \leqq \tfrac{1}{2} z^2(V) - \tfrac{1}{2} z^2(U) + \int_U^V | fz | \, dt.$$

By continuity, (139) holds if $z(V) = z(U) = 0$; that is,

$$c \int_U^V z^2(1 - z) dt \leqq \int_U^V | fz | \, dt.$$

This inequality remains valid if the domain of integration (U, V) is replaced by a sum of open intervals bounded by zeros of $z(t)$ and on which $z > 0$. Since the integral of $z^2(1 - z)$ on a t-set where $z = 0$ is 0, it follows that the last inequality is valid whenever $z(V) = z(U) = 0$ and $z(t) \geqq 0$ on (U, V). Hence (139) is valid for arbitrary intervals $[U, V]$.

If U is so large that $0 \leqq z(t) \leqq \frac{1}{2}$ for $t \geqq U$, then (139) and Hölder's inequality give

$$\tfrac{1}{2}c \int_U^V z^2 dt \leqq \tfrac{1}{2} + \left(\int_U^V |f|^\gamma dt\right)^{1/\gamma} \left(\int_U^V |z|^{\gamma/(\gamma-1)} dt\right)^{1-1/\gamma}.$$

If $\gamma = 1$, then the last integral does not occur and (138_2) follows from the fact that f is of class $L^\gamma = L$. If $\gamma > 1$, then (136_2) implies that $|z|^{\gamma/(\gamma-1)} \leqq z^2$ for large t, and so (138_2) follows from the fact that $1 - 1/\gamma < 1$. This proves Lemma 3.

21. Proof of (i). In order to prove (i), let $y = y(t)$ be a solution of (2) satisfying (115_2), as supplied by (*); cf. (II*) and the remarks following it. To this solution, there belong auxiliary functions $v(t)$ and $w(t)$, given by (128) and (129), which are defined and continuous for large t, satisfy the limit relations (133), and possess continuous derivatives satisfying the differential inequalities (131), (132) on the respective t-sets $\{v(t) \neq 1\}$, $\{w(t) \neq 0\}$.

Condition (114) of (i) and assertion (138) in Lemma 3 imply that

$$\int^\infty w^2 dt < \infty \quad \text{and} \quad \int^\infty (1-v)^2 dt < \infty.$$

From the definitions of v and w, the functions $(M_m/L_{ma})^{\frac{1}{2}}$ and $(N_{m+1}/L_{ma})^{\frac{1}{2}}$ are of class L^2; cf. (134). Since, by condition (113) in (i), there is only one elementary divisor belonging to a λ_j for which $\operatorname{Re}\lambda_j = \mu_m$ and this one is simple, it follows that $L_{ma} = a^2 \,|\, y^m \,|^2$. Hence, y^j/y^m is of class L^2 if $j \neq m$. If $\gamma > 1$, so that $\gamma/(\gamma - 1) > 2$, then (115_2) implies that y^j/y^m is of class $L^{\gamma/(\gamma-1)}$ if $j \neq m$.

The differential equation for y^m in (2) is of the form (15), where $G = \| g_{mj} \|$. Since, for large t, y^m does not vanish,

$$y^{m\prime}/y^m = (\lambda_m + g_{mm}) + \sum_{j \neq m} g_{mj}(y^j/y^m).$$

Thus a quadrature gives

$$y^m(t)/\exp \int^t (\lambda_m + g_{mm}) du = \exp \int^t \sum_{j\neq m} g_{mj}(y^j/y^m) du.$$

If $\gamma = 1$, then, by (114) and (115_2), $g_{mj}(y^j/y^m)$ is of class L; the same holds if $\gamma > 1$, since y^j/y^m is of class $L^{\gamma/(\gamma-1)}$. Thus the expression on the right side of the last formula line tends, as $t \to \infty$, to a non-vanishing constant. If

$y(t)$ is replaced by const. $y(t)$, with a suitable choice of const. $\neq 0$, then (115_1) holds. This proves (i).

22. Proof of (ii). In order to prove (ii), assume the normalizations (72). Introduce the change of independent variables (73) and the successive variations of constants (74), (79) and (83), in which (87) and (88) hold. This transforms (2) into the system (84)-(85), where a differential equation in (84) can be written as (94) or (95) according as $(qk) = (q_0k_0)$ or $(qk) \neq (q_0k_0)$. The assumption (117) of (ii) means that, in the notation of Section 16 above, there is only one pair of indices (q^*k^*), namely, (q_0k_0).

The identities (91) along with the relations (82) and (87) show that the matrix $B = B(s)$ in (84)-(85) is of class L^γ (as a function of s), by virtue of (119). If (III) is used instead of (*) or (II*), then the proof of (i) shows that (84)-(85) has a solution $z = z(s)$ satisfying, as $s \rightarrow \infty$,

$$(140_1) \qquad z^{q_0k_0} \sim \exp \int^s b_{q_0k_0\, q_0k_0} ds,$$

$$(140_2) \qquad z^{jk} = o(|\, z^{q_0k_0}\,|) \quad \text{if} \quad (jk) \neq (q_0k_0).$$

The assumption (119), the identities (91) and the relations (82), (86) show that $t^{h_0 - h(q_0)} b_{q_0k_0\, \alpha\beta}$, where $(\alpha\beta) \neq (q_0k_0)$, is of class L^γ (as a function of s). Since the case $(jk) = (q_0k_0)$ of (94) can be written as

$$(\log z^{q_0k_0})' = b_{q_0k_0\, q_0k_0} + \sum_{(\alpha\beta)\neq(q_0k_0)} \sum b_{q_0k_0\, \alpha\beta} (z^{\alpha\beta}/z^{q_0k_0}),$$

the derivation of (140_1) shows that (140_1) can be improved to

$$(140_1 \text{ bis}) \qquad z^{q_0k_0} = (1 + o(t^{h(q_0) - h_0})) \exp \int^s b_{q_0k_0\, q_0k_0} ds,$$

as $s \rightarrow \infty$.

In view of (77)-(78), (82) and (86),

$$b_{q_0k_0\, q_0k_0} = \sum_{n=1}^{k_0} \sum_{\beta=k}^{h(q_0)} (-1)^{k_0 - n} t^{\beta - n + 1} g_{q_0n\, q_0\beta} / (k_0 - n)!(\beta - k_0)!.$$

Thus, the formulae (120) follow from (73) and (74), (79), (83). This proves (ii).

23. Applications to a second order equation. Let x be a scalar variable. It was shown in [2], pp. 570-573, that if, in the differential equation

$$(141) \qquad x'' - (\lambda + \phi(t))x = 0,$$

λ is a positive constant and $\phi(t)$ is real-valued and continuous for large t, then necessary and sufficient for (141) to be non-oscillatory and to possess a pair of solutions satisfying

$$(142) \qquad x'/x \to \pm\lambda^{\frac{1}{2}} \quad \text{as} \quad t \to \infty$$

is that

$$(143) \qquad \underset{0 \leqq V < \infty}{\text{l. u. b.}} \left| \int_U^{U+V} \phi(t)\,dt \right| / (1 + V) \to 0 \quad \text{as} \quad U \to \infty.$$

The main theorem (*) of Part II gives an immediate extension of one half of this theorem to the case when λ is a complex number, but is not negative or 0, and $\phi(t)$ is allowed to be complex-valued. (For an analogous theorem when λ is a negative number and $\phi(t)$ is real-valued, cf. [4].)

(a) *Let λ be a complex number such that*

$$(144) \qquad \operatorname{Re} \lambda^{\frac{1}{2}} \neq 0$$

and let $\phi(t)$ be a continuous complex-valued function satisfying

$$(145) \qquad \underset{0 \leqq V < \infty}{\text{l. u. b.}} \int_U^{U+V} |\phi(t)|\,dt/(1 + V) \to 0 \quad \text{as} \quad U \to \infty.$$

Then (141) *has a pair of solutions which do not vanish for large t and satisfy* (142).

In order to prove (a), write (141) as a first order system $y' = (J + G(t))y$ for the vector $y = (y^1, y^2)$, where

$$(146) \qquad y^1 = x' + \lambda^{\frac{1}{2}}x, \qquad y^2 = x' - \lambda^{\frac{1}{2}}x,$$

for some fixed choice of the square root $\lambda^{\frac{1}{2}}$. It is readily verified that (146) satisfies $y' = (J + G(t))y$, where

$$(147) \qquad J = \begin{pmatrix} \lambda^{\frac{1}{2}} & 0 \\ 0 & -\lambda^{\frac{1}{2}} \end{pmatrix} \text{ and } G(t) = \tfrac{1}{2}\lambda^{-\frac{1}{2}}\phi \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix}.$$

Conditions (144), (145) imply conditions (54), (6) of (II*), respectively. Hence (II*) implies the existence of a solution $y = (y^1(t), y^2(t))$ satisfying

$$(148) \qquad y^1(t) = o(|y^2(t)|) \quad \text{as} \quad t \to \infty.$$

The corresponding solution $x = x(t)$ of (141) satisfies, by (146),

$$(1 + o(1))x' = (\lambda^{\frac{1}{2}} + o(1))x \quad \text{as} \quad t \to \infty;$$

that is, $x'/x \to \lambda^{\frac{1}{2}}$. Since the choice of $\lambda^{\frac{1}{2}}$ is arbitrary, assertion (a) follows.

Theorem (VII) in [2], p. 575, which deals with the case $\lambda = 1$ and a real-valued $\phi = \phi(t)$, can be extended as follows:

(β) *If* (144) *holds and* (145) *is strengthened to*

$$(149) \qquad \int^{\infty} |\phi(t)|^{\gamma}\, dt < \infty \text{ for some } \gamma, \text{ where } 1 \leqq \gamma \leqq 2,$$

then (141) *has a pair of solutions satisfying* (142) *and*

$$(150) \qquad x \sim \exp \pm \int^{t} (\lambda^{\frac{1}{2}} + \tfrac{1}{2}\lambda^{-\frac{1}{2}}\phi(u))du \quad \text{as} \quad t \to \infty.$$

If, in addition, $\phi(t)$ is (improperly) integrable at $t = \infty$, that is, if

$$\int^{\infty} \phi(t)dt = \lim_{T\to\infty} \int^{T} \phi(t)dt \text{ exists},$$

then (150) can be replaced by $x \sim \exp(\pm \lambda^{\frac{1}{2}} t)$.

The assertions of (β) follow from (i), since (i) supplies the existence of a vector (146) satisfying (148) and

$$y^1 \sim \text{const.} \exp \int^{t} (\lambda^{\frac{1}{2}} + \tfrac{1}{2}\lambda^{-\frac{1}{2}}\phi(u))du,$$

where const. $\neq 0$ can be chosen to be $2\lambda^{\frac{1}{2}}$.

Cf. (vi) and (vii) in [6], p. 722, for the analogues of (α) and (β) when $\lambda = 0$. It is clear from (α) and (β) that the theorems (vi), (vii) in [6] have analogues when the coefficient function $f(t)$ there is complex-valued.

24. Applications to a second order equation (continued). There will now be considered theorems of the type (α), (β) in which (141) is replaced by

$$(151) \qquad x'' - f(t)x = 0,$$

and it is not assumed that $f(t)$ is "nearly constant" for large t. The analogue of (α) is as follows:

(γ) *Let $f(t)$ be a continuous (possibly complex-valued) function for large t satisfying*

$$(152_1) \quad \operatorname{Re} f^{\frac{1}{2}}(t) \neq 0; \qquad (152_2) \quad \int^{\infty} |\operatorname{Re} f^{\frac{1}{2}}(t)|\, dt = \infty.$$

In addition, suppose that $f(t)$ has a continuous derivative satisfying

$$(153) \qquad f'(t) = o(|f(t)|\cdot|\operatorname{Re} f^{\frac{1}{2}}(t)|) \quad \text{as} \quad t \to \infty.$$

Then (151) *has a pair of solution satisfying*

$$(154) \qquad x'(t) \sim \pm f^{\frac{1}{2}}(t)x(t) \quad \text{as} \quad t \to \infty.$$

If condition (152_1) is replaced by $|\arg f(t)| < \text{const.} < \pi$ for large t, then (153) is equivalent to $f' = o(|f|^{\frac{3}{2}})$ as $t \to \infty$. When $f(t)$ is real-valued (hence positive), the condition that $f(t)$ is continuously differentiable can be omitted and (153) can be relaxed to

$$(155) \qquad \underset{0 \leqq V < \infty}{\text{l.u.b.}} |\log f(U+V)/f(U)|/(1 + \int_U^{U+V} f^{\frac{1}{2}}(t)dt) \to 0 \quad \text{as} \quad U \to \infty.$$

In fact, when (152) holds with $f = \operatorname{Re} f$, then (155) is necessary and sufficient for (151) to be non-oscillatory and to possess a pair of solutions satisfying (154). These assertions will be clear from the proof of (γ) and the proof of (IV) in [2], pp. 570-573.

In the proof of (γ), the condition

$$(156) \qquad \underset{0 \leqq V < \infty}{\text{l.u.b.}} \left(\int_U^{U+V} |df(t)/f(t)|\right)/(1 + \int_U^{U+V} |\operatorname{Re} f^{\frac{1}{2}}(t)|\, dt) \to 0 \text{ as } U \to \infty$$

will be used, rather than the more stringent condition (153).

The analogue of (β) is the following:

(δ) *If condition* (153) *in* (γ) *is replaced by*

$$(157) \qquad \int^{\infty} |f'/f|^{\gamma}\, |\operatorname{Re} f^{\frac{1}{2}}|^{\gamma-1}\, dt < \infty \text{ for some } \gamma, \text{ where } 1 \leqq \gamma \leqq 2,$$

then (151) *has a pair of solutions satisfying* (154) *and*

$$(158) \qquad x(t) \sim f^{-\frac{1}{4}}(t) \exp \pm \int^t f^{\frac{1}{2}}(u)du \quad \text{as} \quad t \to \infty.$$

In (157)-(158), as well as (154) above, $f^{\frac{1}{2}}(t)$ denotes a fixed continuous determination of the square root of f. Similarly, $f^{-\frac{1}{4}}(t)$ in (158) is a continuous square root of $1/f^{\frac{1}{2}}$.

The asymptotic formulae (158) were obtained in [10] under conditions quite different from (157). The conditions of [10] require that $f(t)$ be real-valued and either positive or negative (the latter case is eliminated from (δ) by condition (152_1) and that $f(t)$ should have a continuous second derivative satisfying (166) below.

In order to prove (γ), let $y = (y^1, y^2)$ denote the vector with the components

$$(159) \qquad y^1 = x' + f^{\frac{1}{2}}x, \qquad y^2 = x' - f^{\frac{1}{2}}x,$$

where $f^{\frac{1}{2}}$ denotes a fixed continuous determination of the square root of f. By (159),

$$(160) \qquad x = \tfrac{1}{2}f^{-\frac{1}{2}}(y^1 - y^2), \qquad x' = \tfrac{1}{2}(y^1 + y^2).$$

Thus (151) is equivalent to the linear system

$$y^{1\prime} = f^{\frac{1}{2}}y^1 + f'(y^1 - y^2)/4f, \qquad y^{2\prime} = -f^{\frac{1}{2}}y^2 - f'(y^1 - y^2)/4f$$

of first order for y (where $f'/f = 2(f^{\frac{1}{2}})'/f^{\frac{1}{2}}$). Introduce the new independent variable defined by

$$(161) \qquad s = \int^t g(t)\,dt, \quad \text{where} \quad g = |\operatorname{Re} f^{\frac{1}{2}}|, \qquad (ds = g\,dt).$$

Then $t \to \infty$ is equivalent to $s \to \infty$, by virtue of (152_2). If a dot denotes differentiation with respect to s, then the system for y becomes $\dot{y} = (J(t) + G(t))y$, where $t = t(s)$ and

$$J(t) = \begin{pmatrix} f^{\frac{1}{2}}/g & 0 \\ 0 & -f^{\frac{1}{2}}/g \end{pmatrix} \text{and } G(t) = (f'/4fg)\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}.$$

Since $|\operatorname{Re}(f^{\frac{1}{2}}/g + f^{\frac{1}{2}}/g)| = 2 \neq 0$, condition (54) of (II*) is satisfied. In terms of s, condition (6) of (II*) is implied by (154) or (156). Thus there exist solutions $x = x(t)$ of (151) satisfying, as $t \to \infty$,

$$(162) \qquad y^1 = o(y^2) \quad \text{or} \quad y^2 = o(y^1).$$

In view of (160), this proves assertion (154) of (γ).

[*Added in the proofs*, 12. 1. 1954. After the transformation of the differential equation (151) of second order into the binary system of first order in the formula line following (160), the assertion (γ) could also be deduced from a theorem of Z. Szmydtówna, Ann. de la Soc. Polonaise de Math., vol. 24 (1951), pp. 17-34.]

In order to prove (δ), note that (157) and (161) imply that $|G(t)|^\gamma$, as a function of s, is of class L. Hence Theorem (i) in Section 18 states that (151) has solutions $x = x(t)$ satisfying (154) and

$$y^1(t) \sim 2\exp\int^t (f^{\frac{1}{2}}(u) + f'(u)/4f(u))\,du,$$

$$y^2(t) \sim 2\exp\int^t (-f^{\frac{1}{2}}(u) + f'(u)/4f(u))\,du.$$

Since the latter two formulae can be written as

$$y^1(t) \sim 2f^{\frac{1}{4}}(t) \exp \int^t f^{\frac{1}{2}}(u)\,du, \qquad y^2(t) \sim 2f^{\frac{1}{4}}(t) \exp \int^t -f^{\frac{1}{2}}(u)\,du,$$

assertion (δ) follows from (159) and (161).

Another theorem leading to asymptotic formulae for the solutions of (151) is the following:

(ϵ) *Let $f(t)$ satisfy the conditions of* (γ). *In addition, let $f'/f^{\frac{3}{2}}$ be of bounded variation for large t, that is, let*

$$\int^\infty |\, d(f'/f^{\frac{3}{2}}) \,| < \infty. \tag{163}$$

Then (151) *has a pair of solutions satisfying* (154) *and*

$$x(t) \sim f^{-\frac{1}{4}}(t) \exp \pm \int^t f^{\frac{1}{2}}(1 + f'^2/16f^3)^{\frac{1}{2}} dt \quad \text{as} \quad t \to \infty. \tag{164}$$

In view of (153), $f'^2/f^3 \to 0$ as $t \to \infty$. The square root in $(1 + f'^2/16f^3)^{\frac{1}{2}}$ can be chosen so that $(1 + f'^2/16f^3)^{\frac{1}{2}} \to 1$ as $t \to \infty$; the determinations of $f^{\frac{1}{2}}$ and $f^{-\frac{1}{4}}$ are chosen as in (158).

If $f(t)$ has a continuous second derivative, condition (163) means that

$$\int^\infty |\, f''/f^{\frac{3}{2}} - 3f'^2/2f^{\frac{5}{2}} \,|\, dt < \infty. \tag{165}$$

The condition in [10] for the validity of (158) (rather than (164)) is

$$\int^\infty |\, f''/f^{\frac{3}{2}} - 5f'^2/4f^{\frac{5}{2}} \,|\, dt < \infty \tag{166}$$

(when $f(t) \neq 0$ is real-valued).

In order to prove (ϵ), note that (γ) is applicable, hence (151) has solutions satisfying (154). Let $x = x(t)$ be a solution of (151) which satisfies

$$v(t) \to 1 \quad \text{as} \quad t \to \infty, \tag{167}$$

where

$$v = x'/f^{\frac{1}{2}}x. \tag{168}$$

It is readily verified that (168) satisfies the Riccati equation

$$v' + v^2 f^{\frac{1}{2}} + \tfrac{1}{2} f' f^{-1} v - f^{\frac{1}{2}} = 0,$$

by virtue of (151). This can be written as

$$v' + f^{\frac{1}{2}}\{(v + f'/4f^{\frac{3}{2}})^2 - (1 + f'^2/16f^3)\} = 0,$$

or as

$$(169)\qquad f^{\frac{1}{2}}\{(v + f'/4f^{\frac{3}{2}}) - (1 + f'^2/16f^3)^{\frac{1}{2}}\} = -v'/(v + a(t)),$$

where

$$(170)\qquad a(t) = f'/4f^{\frac{3}{2}} + (1 + f'^2/16f^3)^{\frac{1}{2}}.$$

Note that $a(t) \rightarrow 1$ as $t \rightarrow \infty$, by the above normalizations of the square roots; so that $v(t) + a(t) \rightarrow 2$ as $t \rightarrow \infty$, by (167).

Let v on the left of (169) be written as $x'/f^{\frac{1}{2}}x$ (cf. (168)). Then a quadrature shows that

$$x(t)f^{\frac{1}{4}}(t)/\exp \int^t f^{\frac{1}{2}}(u)(1 + f'^2(u)/16f^3(u))^{\frac{1}{2}}du$$

is equal to

$$(a(t) + v(t))^{-1} \exp \int^t (v(u) + a(u))^{-1} da(u).$$

This is clear if $v'dt$ is written as $d(v + a) - da$. The expression in the last formula line tends to a limit, as $t \rightarrow \infty$, since $(a(t) + v(t))^{-1}$ does and since $a(u)$ is of bounded variation. Thus if const. $x(t)$, for a suitable choice of const., is renamed $x(t)$, it is clear that (164) holds when $+$ is written in place of $\pm$. Since the choice of the square root $f^{\frac{1}{2}}$ in (168) was arbitrary, (ϵ) is proved.

25. An elliptic analogue. Assertions (β) or (δ) have no analogues when λ is a negative constant or $f(t)$ is negative for large t, respectively. As to (β), cf. the example in [11], p. 269. On the other hand, (ϵ) does have an analogue in the "elliptic" case.

(η) *Let $f(t)$ be a non-vanishing (possibly complex-valued) function for large t having a continuous derivative satisfying* (163) *and*

$$(171)\qquad \lim_{t\rightarrow\infty} f'^2/16f^3 \neq -1.$$

Suppose further that

$$(172)\qquad \exp \pm i \int^t f^{\frac{1}{2}}(1 + f'^2/16f^3)^{\frac{1}{2}}du = O(1) \quad \text{as} \quad t \rightarrow \infty.$$

Then the differential equation

$$(173)\qquad x'' + f(t)x = 0$$

has a pair of solutions satisfying, as $t \rightarrow \infty$,

$$(174)\qquad x \sim f^{-\frac{1}{4}}(t) \exp \pm i \int^t f^{\frac{1}{2}}(1 + f'^2/16f^3)^{\frac{1}{2}}du$$

and

$$x' \sim (-\alpha^{\frac{1}{2}} \pm i(1+\alpha)^{\frac{1}{2}})f^{\frac{1}{2}}x, \tag{175}$$

where α *is the limit in* (171).

Conditions (171)-(172) are trivially satisfied if $f(t)$ is (real and) positive for large t. As in the above theorems, all powers of $f(t)$ which occur can be assumed to be integral (positive or negative) powers of a fixed fourth root $f^{\frac{1}{4}}(t)$; in such a normalization, $\alpha^{\frac{1}{2}}$ in (175) is the limit, as $t \to \infty$, of $(f^{\frac{1}{4}})'/f^{\frac{3}{4}}$.

The proof of (η) will depend on the simplest case, $J = 0$, of Theorem (**) in Part II and will be like the procedure used in [11], pp. 262-263, for similar purposes.

In the proof of (η), there is no actual loss of generality in the (local) assumption that $f(t)$ has a continuous second derivative; so that (163) is equivalent to (165). The variation of constants

$$z = xf^{\frac{1}{4}} \tag{176}$$

transforms (173) into

$$(f^{-\frac{1}{2}}z')' + (f^{\frac{1}{2}}(t) + a(t))z = 0, \tag{177}$$

where

$$a(t) = f''/4f^{\frac{3}{2}} - 5f'^2/16f^{\frac{5}{2}}. \tag{178}$$

If $y = (y^1, y^2)$, where

$$y^1 = z, \qquad y^2 = f^{-\frac{1}{2}}z', \tag{179}$$

then (177) is equivalent to the system

$$\overset{\bullet}{y}' = A(t)y, \quad \text{where} \quad A(t) = \begin{pmatrix} 0 & f^{\frac{1}{2}} \\ -f^{\frac{1}{2}} - a & 0 \end{pmatrix}. \tag{180}$$

If z denotes either of the functions on the left of (172) and if

$$(\cdot\ \cdot\ \cdot) = (1 + f'^2/16f^3), \tag{181}$$

then $z' = \pm if^{\frac{1}{2}}(\cdot\ \cdot\ \cdot)^{\frac{1}{2}}z$, and so $(f^{-\frac{1}{2}}z')' = -(\cdot\ \cdot\ \cdot)f^{\frac{1}{2}}z \pm i\{(\cdot\ \cdot\ \cdot)^{\frac{1}{2}}\}'z$. If $\pm iz$ in the last term is replaced by $z'f^{-\frac{1}{2}}(\cdot\ \cdot\ \cdot)^{-\frac{1}{2}}$, it is seen that the functions on the left of (172) are solutions of the differential equation

$$(f^{-\frac{1}{2}}z') - \tfrac{1}{2}f^{-\frac{1}{2}}(\cdot\ \cdot\ \cdot)^{-1}(\cdot\ \cdot\ \cdot)'z' + (\cdot\ \cdot\ \cdot)f^{\frac{1}{2}}z = 0. \tag{182}$$

Let $w = (w^1, w^2)$, where

$$w^1 = z, \qquad w^2 = f^{-\frac{1}{2}}z'; \tag{183}$$

so that (182) is equivalent to the system

$$(184)\qquad w' = B(t)w, \text{ where } B(t) = \begin{pmatrix} 0 & f^{\frac{1}{2}}(t) \\ -(\cdot\cdot\cdot)f^{\frac{1}{2}} & \frac{1}{2}(\cdot\cdot\cdot)^{-1}(\cdot\cdot\cdot)' \end{pmatrix}.$$

In view of the derivation of the differential equation (182), a fundamental matrix for (182) is

$$(185)\qquad W(t) = \begin{pmatrix} w_1{}^1(t) & w_2{}^1 \\ -i(\cdot\cdot\cdot)^{\frac{1}{2}}w_1{}^1 & i(\cdot\cdot\cdot)w_2{}^1 \end{pmatrix},$$

where

$$(186)\qquad w_j{}^1 = \exp(-1)^j i \int^t f^{\frac{1}{2}}(1 + f'^2/16f^3)^{\frac{1}{2}}du, \qquad j = 1, 2,$$

are the functions in (172).

The variation of constants

$$(187)\qquad y = W(t)v$$

transforms (180) into

$$(188)\qquad v' = W^{-1}(A - B)Wv.$$

In view of (178), (180), (181) and (184),

$$A - B = \begin{pmatrix} 0 & 0 \\ 3f'^2/8f^{\frac{5}{2}} - f''/4f^{\frac{3}{2}} & -\frac{1}{2}(\cdot\cdot\cdot)^{-1}(\cdot\cdot\cdot)' \end{pmatrix}.$$

The assumption (163) implies that the elements of $A - B$ are of class L (cf. (165)), while the condition (172) implies that $W(t) = O(1)$ as $t \to \infty$. Since $\det W(t) = 2i(\cdot\cdot\cdot)$, it follows that $(\det W(t))^{-1}$, and therefore $W^{-1}(t)$, is $O(1)$, as $t \to \infty$. Thus the coefficients of the system (188) are of class L for large t. Hence, the simplest case, $J = 0$, of (**) states that (188) has a solution satisfying, as $t \to \infty$,

$$(189)\qquad v^1(t) \to 1 \quad\text{and}\quad v^2(t) \to 0,$$

and another solution satisfying, as $t \to \infty$,

$$(190)\qquad v^1(t) \to 0 \quad\text{and}\quad v^2(t) \to 1.$$

The solution $y = y(t)$ of (180) corresponding to (189), by virtue of (187), satisfies

$$y^1(t) \sim w_1{}^1(t), \qquad y^2(t) \sim -i(\cdot\cdot\cdot)^{\frac{1}{2}}w_1{}^1$$

as $t \to \infty$. In view of (176) and (179), the corresponding solution $x = x(t)$ of (173) satisfies

$$f^{\frac{1}{4}}x \sim w_1{}^1, \qquad f^{-\frac{1}{4}}(xf^{\frac{1}{4}})' \sim -i(\cdot\cdot\cdot)^{\frac{1}{2}}w_1{}^1$$

as $t \to \infty$. The second of these relations reduces, by virtue of the first, to

$$x' = (1 + o(1))\{-f'/4f^{\frac{3}{2}} - i(\cdot\ \cdot\ \cdot)^{\frac{1}{2}}\}f^{\frac{1}{2}}x.$$

The last two formula lines prove the case — of $\pm$ in (174), (175). The other case results from (190). This proves (η).

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] O. Dunkel, "Regular singular points of a system of homogeneous linear differential equations of the first order," *Proceedings of the American Academy of Arts and Sciences*, vol. 38 (1902-03), pp. 341-370.

[2] P. Hartman, "Unrestricted solution fields of almost separable differential equations," *Transactions of the American Mathematical Society*, vol. 63 (1948), pp. 560-580.

[3] ———, "On non-oscillatory linear differential equations of second order," *American Journal of Mathematics*, vol. 74 (1952), pp. 389-400.

[4] ——— and A. Wintner, "The asymptotic arcus variation of solutions of real linear differential equations of second order," *ibid.*, vol. 70 (1948), pp. 1-10.

[5] ——— and A. Wintner, "On non-linear differential equations of first order," *ibid.*, vol. 72 (1950), pp. 347-358.

[6] ——— and A. Wintner, "On non-oscillatory differential equations," *ibid.*, vol. 75 (1953), pp. 717-730.

[7] F. Lettenmeyer, "Ueber das asymptotische Verhalten der Lösungen von Differentialgleichungen und Differentialgleichungssystemen," *Sitzungsberichte München*, 1929, pp. 201-252.

[8] O. Perron, "Über Stabilität und asymptotisches Verhalten der Integrale von Differentialgleichungssystemen," *Mathematische Zeitschrift*, vol. 29 (1929), pp. 129-160.

[9] ———, "Die Ordnungszahlen linearer Differentialgleichungssysteme," *ibid.*, vol. 31 (1930), pp. 748-766.

[10] A. Wintner, "On the normalization of characteristic differentials in continuous spectra," *Physical Review*, vol. 72 (1947), pp. 516-517.

[11] ———, "Asymptotic integrations of the adiabatic linear oscillator," *American Journal of Mathematics*, vol. 69 (1947), pp. 251-272.

QUADRATIC FORMS OVER LOCAL FIELDS.*

By O. T. O'Meara.

Introduction. Even after Minkowski had *solved* the problem of equivalence of quadratic forms the matter was by no means *settled,* for the invariants found in [17] are intricate both in their derivation and application. The difficulties presented (even in the theory of rational equivalence) were largely due to the use of integral forms and the problem was simplified by Hasse [5] who rid it of its integral considerations, solved the problem of fractional equivalence in the p-adic numbers and tied them together to form a complete system of invariants under rational equivalence in the large; he related these invariants to those of Minkowski. In the subsequent paper [6], Hasse extended his results to quadratic forms over algebraic number fields and their local completions. These results were in turn extended by Witt's using the theory of algebras in [20]. Kaplansky showed in [13] that Witt's invariants apply to fields F which are not formally real and for which $F^*/(F^*)^2$ has order 4.

The problem of tackling the original theory of integral equivalence remained, but use could now be made of the results on fractional equivalence proved independently of it. Siegel [18] proved a conjecture of Minkowski that two rational integral forms are in the same genus if and only if they are semi-equivalent; Jones [7] proved that the Witt cancellation law [20] holds under integral equivalence over the p-adic numbers (p odd) and stated that the result also held for arbitrary local fields in which $|2|=1$; Durfee [3, 4] gave a complete set of invariants and a simple proof of the Witt cancellation law for integral forms in these fields; Jones [8] showed how to determine when two forms over the 2-adic integers are equivalent and this was expressed by Pall [15] in the form of invariants; most of these results can be found in coordinated form (but over the rational p-adic numbers only) in [9].

Eichler employed the more geometrical notion of lattices to discuss the local theory in [11, Chapter II]: of particular interest to us will be his results on the equivalence of maximal forms. Eichler [12] and Kneser [14] proved the Witt cancellation law for positive definite forms over the rational integers.

* **Received August 26, 1953; revised June 8, 1954 and September 15, 1954.**

In the present paper we are concerned with integral equivalence over local fields and the previous remarks show that the only local cases requiring real investigation are those in which $|2|<1$. We prove a weak form of cancellation law for these fields: that this cannot be fully generalized is clear from the counter-example in [3]. Certain useful type invariants are given in the general case, but these do not form a complete set under integral equivalence. However a characterization is given over local fields in which 2 is a prime; this is facilitated by the use of lattices but the real key seems to lie in the perfectness of the residue class field. The ramified case is much more complicated than this and simple examples show that we cannot expect the same answers as in the unramified theory; the numbers represented by the form seem to play an important role; the perfectness of the residue class field pulls us through again and we can characterize forms of unit determinant, but the problem remains of finding a complete set of invariants for forms of arbitrary determinant over a general local field.

1. Preliminary definitions. In the present paper we consider quadratic forms over local fields, that is to say over fields which are complete under a discrete non-Archimedean valuation and have a perfect residue class field [1]. F will denote the local field, $\mathfrak{o}$ the ring of integers in F and π will be a fixed prime element in F. We define $e=\operatorname{ord}(2)$ as the ramification index of F. We assume in addition that F does not have characteristic 2. To avoid the use of an excessive number of multipliers we introduce the following notation: a specific element $a\pi^t$ will sometimes be written as $[\pi^t]$ if $|a|=1$ or as $\{\pi^t\}$ if $a\in\mathfrak{o}$. Thus, if $\alpha=[\pi^t]$, $\beta=[\pi^t]$ and $\gamma=\{\pi^t\}$, α need not be equal to β but we must have $|\gamma|\leqq|\alpha|=|\beta|$.

If R is an n-dimensional vector space over F, we call an $\mathfrak{o}$-module L in R a lattice if there is a basis for R in which L can be expressed as $L=\mathfrak{o}\xi_1+\cdots+\mathfrak{o}\xi_n$ [see 11, p. 47]. We call (ξ) a minimal basis for L and note that L may very well have many minimal bases.

Now let l be a quadratic form and $\Lambda=(l_{ij})$ its corresponding matrix. By fixing a basis (ξ) for R we can make R into a metric space V by defining $\xi_i\cdot\xi_j=l_{ij}=l_{ji}=\xi_j\cdot\xi_i$, [20, p. 32]. The form k is fractionally equivalent to l if and only if there is another basis (η) for V in which $k_{ij}=\eta_i\cdot\eta_j$. We then write $l\sim k$. Conversely we can associate a quadratic form with a given metric space V by fixing a basis (ξ) for V and defining $l_{ij}=\xi_i\cdot\xi_j$.

Now let $l\sim k$ have respective bases (ξ) and (η) in V and consider the lattices $L=\mathfrak{o}\xi_1+\cdots+\mathfrak{o}\xi_n$ and $K=\mathfrak{o}\eta_1+\cdots+\mathfrak{o}\eta_n$. Then L and K are integrally equivalent (written $L\cong K$) if and only if there are minimal

bases (ξ') and (η') for L and K respectively such that $\xi_i' \cdot \xi_j' = \eta_i' \cdot \eta_j'$, and this in turn is equivalent to saying that there is an isometry $V \to V$ which carries L onto K. If L and K are isometric we write $L \cong K$, $l \cong k$ and $\Lambda \cong \mathrm{K}$. We denote the fact that l is associated with L by writing $l \cong L \cong \Lambda$. We call $\det(l_{ij})$ the determinant of L and write it as $d(L)$; this is unique but for a factor which is the square of a unit. We assume that all forms are non-degenerate: $\det(l_{ij})$ unequal to zero.

L is the orthogonal sum of sublattices L_1 and L_2, written $L = L_1 \oplus L_2$, if $L_1 \cap L_2 = 0$, L_1 is orthogonal to L_2, and L_1 and L_2 together span L. It is easy to see that if $L = L_1 \oplus K_2$ then $K_2 = L_2$.

The ideal generated by X^2 as X runs through L will be called the norm of L and written $N(L)$. L is said to be integral if $N(L) \subseteq \mathfrak{o}$: if L is integral, then $X \cdot Y \varepsilon (\frac{1}{2}) \cdot \mathfrak{o}$ for all X and Y in L. If in addition $X \cdot Y \varepsilon \mathfrak{o}$ for all X and Y in L, we say that L is totally integral.

I. Lattices Over Local Fields.

In this chapter we discuss type invariants, lattices of unit determinant and the cancellation law. In general the fields considered will be local fields but it will be necessary to indicate certain modifications for different values of e.

2. Canonical representation of a lattice. Our aim is to show that every lattice $L = \mathfrak{o}\xi_1 + \cdots + \mathfrak{o}\xi_n$ can be expressed in an almost orthogonal canonical basis.

Definition 2.1. $\xi_1, \cdots, \xi_n$ is a canonical basis for L if

(1) when $e = 0$: $\xi_i \cdot \xi_j = 0$ for all $i \neq j$; and $|\xi_i^2| \geqq |\xi_{i+1}^2|$.

(2) when $e \geqq 1$: (a) $\xi_i \cdot \xi_j \neq 0$ and $i \neq j$ happens in at most one of the cases $j = i - 1$ or $j = i + 1$; and $\xi_i \cdot \xi_j$ is then an exact power of π; (b) $\max |\xi_i \cdot Z| \geqq \max |\xi_{i+1} \cdot Z|$, $Z \varepsilon L$, $1 \leqq i \leqq n - 1$; (c) if $\max |\xi_i \cdot Z| = |\xi_j^2| = \max |\xi_j \cdot Z|$, $Z \varepsilon L$, holds for a particular value of i and a particular value of j (which may be equal to i), then that ξ_i is orthogonal to all ξ_k, $k \neq i$, and so $|\xi_i^2| = \max |\xi_i \cdot Z| = |\xi_j^2|$. Observe that (a), (b) and (c) imply that if $\xi_i \cdot \xi_{i+1} \neq 0$ then $|\xi_i^2| < |\xi_i \cdot \xi_{i+1}|$ and $|\xi_{i+1}^2| < |\xi_i \cdot \xi_{i+1}|$.

We now prove some results for the lattice L expressed in any basis (ξ).

LEMMA 2.1. *If* $|\xi_1^2| = \max |\xi_1 \cdot \xi_i|$, *then there is a sublattice* L_1 *of* L *such that* $L = \mathfrak{o}\xi_1 \oplus L_1$.

Proof. Replace ξ_i by $\Xi_i = (\xi_i - (\xi_1 \cdot \xi_i)/\xi_1^2 \cdot \xi_1)$ for all $1 < i \leqq n$. Since $\xi_1 \cdot \xi_i/\xi_1^2$ is an integer it follows that $L = \mathfrak{o}\xi_1 + \mathfrak{o}\Xi_2 + \cdots + \mathfrak{o}\Xi_n$. The remark $\xi_1 \cdot \Xi_i = 0$ completes the proof.

LEMMA 2. 2. *If the equations* $\xi_1 \cdot \xi_i + \alpha_i \xi_1^2 + \beta_i(\xi_1 \cdot \xi_2) = 0$ *and* $\xi_2 \cdot \xi_i + \alpha_i(\xi_1 \cdot \xi_2) + \beta_i \xi_2^2 = 0$ *have a simultaneous integral solution* (α_i, β_i) *for all* $2 < i \leqq n$, *then there is a sublattice* L_1 *of* L *such that* $L = (\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2) \oplus L_1$.

Proof. Replace each ξ_i, $2 < i \leqq n$, by $\Xi_i = \xi_i + \alpha_i \xi_1 + \beta_i \xi_2$, and write $L = (\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2) \oplus (\mathfrak{o}\Xi_3 + \cdots + \mathfrak{o}\Xi_n)$. Q. E. D.

LEMMA 2. 3. *Let* $e > 0$. *If* L *is a totally integral lattice of unit determinant and if* $N(L) = \mathfrak{o}$, *then* L *has an orthogonal basis.*

Proof. Induction to n. Since $N(L) = \mathfrak{o}$ there must be a ξ_i (call it ξ_1) such that ξ_1^2 is a unit. Use Lemma 2. 1 and write $L = \mathfrak{o}\xi_1 \oplus L_1$. If $N(L_1) = \mathfrak{o}$, we are through. If $N(L_1) \subseteq (\pi) \cdot \mathfrak{o}$, let ξ_2, ξ_3 be two basis elements of L_1 such that $\xi_2 \cdot \xi_3$ is a unit (two such vectors must exist since $d(L_1)$ is a unit); L_1 must necessarily be of the form $(\mathfrak{o}\xi_2 + \mathfrak{o}\xi_3) \oplus L_2$ since $|\xi_2 \cdot \xi_3| = 1$, $\xi_2^2 \varepsilon (\pi) \cdot \mathfrak{o}$, $\xi_3^2 \varepsilon (\pi) \cdot \mathfrak{o}$ allows integral solutions for the equations of Lemma 2. 2. Then

$$\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2 + \mathfrak{o}\xi_3 = \mathfrak{o}(\xi_2 + \xi_1) + \mathfrak{o}\xi_3 + \mathfrak{o}\xi_1 = (\mathfrak{o}(\xi_2 + \xi_1) + \mathfrak{o}\xi_3) \oplus \mathfrak{o}\eta,$$

again in virtue of Lemma 2. 2. Hence $L = \mathfrak{o}\eta \oplus L_1^*$ with $(\xi_2 + \xi_1) \varepsilon L_1^*$; that is, $N(L_1^*) = \mathfrak{o}$. Induction completes the proof.

THEOREM 2. 4. *L has a canonical basis.*

Proof. Induction to n. There is no loss of generality if we assume that L is totally integral and contains an X and a Y for which $X \cdot Y$ is a unit. If $e = 0$ this implies that there is a basis in which ξ_1^2 (say) is a unit.

Case 1. $N(L) = \mathfrak{o}$. By the previous remark this includes the case $e = 0$ and there is a ξ_1 such that $|\xi_1^2| = 1$. If $e \geqq 1$ there must still be a ξ_1 (say) such that $|\xi_1^2| = 1$ else $N(L)$ would not be $\mathfrak{o}$. Then Lemma 2. 1 entitles us to write $L = \mathfrak{o}\xi_1 \oplus L_1$. The inductive assumption allows us to express L_1 in a canonical basis in such a way that $L_1 = L_1^* \oplus L_1^{**}$ where L_1^* is of unit determinant and $|X \cdot Y| < 1$ for all X and Y in L_1^{**}. By the induction when $e = 0$, and by Lemma 2. 3 when $e \geqq 1$, $\mathfrak{o}\xi_1 \oplus L_1^*$ must have an orthogonal basis $\eta_1, \cdots, \eta_i$ with the property $|\eta_j^2| = 1$ for all $1 \leqq j \leqq i$; and L_1^{**} has a canonical basis $\eta_{i+1}, \cdots, \eta_n$. Then

$$L = (\mathfrak{o}\eta_1 + \cdots + \mathfrak{o}\eta_i) \oplus (\mathfrak{o}\eta_{i+1} + \cdots + \mathfrak{o}\eta_n)$$

is the basis required for L.

Case 2. $N(L) \subseteq (\pi) \cdot \mathfrak{o}$. Let $|\xi_1 \cdot \xi_2| = 1$ (say). Then $\xi_1^2 \varepsilon (\pi) \cdot \mathfrak{o}$ and we can therefore apply Lemma 2.2 to express $L = (\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2) \oplus L_1$, replacing ξ_1 by $\xi_1/(\xi_1 \cdot \xi_2)$ if necessary in order to ensure that $\xi_1 \cdot \xi_2 = \pi^0$. Induction yields the result and the proof is therefore complete.

Of course L will have many canonical bases, but we aim to show that it can be characterized in terms of invariants attached to an arbitrary canonical basis provided that $e \leqq 1$. Lemmas 2.1 and 2.2 are of practical importance; they are proved in [11, Satz 9.2] but the canonical form established there is not the same as ours and need not satisfy definition 2.1, (b) and (c).

Having expressed L in a canonical basis we can write

$$(2.1) \quad L = L_1(\pi^{s(1)}) \oplus L_2(\pi^{s(2)}) \oplus \cdots \oplus L_r(\pi^{s(r)}) \text{ with } s(i) < s(i+1)$$

where $L_j(\pi^{s(j)})$ is the sublattice spanned by these ξ_i for which $\max |\xi_i \cdot Z| = |\pi^{s(j)}|$; then $L_j \cong \pi^{s(j)} \cdot l_j$ where l_j is totally integral, of unit determinant and either of the form $\sum[1]$ or $\sum\begin{pmatrix} \{\pi\} & 1 \\ 1 & \{\pi\} \end{pmatrix}$; and $s(1) < s(2) \cdots < s(r)$.

Definition 2.2. $L_m(\pi^{s(m)})$ is a proper lattice if $N(L_m) = (\pi^{s(m)}) \cdot \mathfrak{o}$; otherwise improper.

A glance at the determinant of L_m together with Theorem 2.4 shows that L_m has an orthogonal basis if and only if it is proper; if improper, L_m is the orthogonal sum of indecomposable lattices of dimension precisely 2. Improper lattices do not occur when $e = 0$.

3. Invariance of type. In order to be able to attach certain well-defined quantities to L we first prove the following theorem which we have already shown to hold for lattices of unit determinant. Compare the weaker result [3, Lemma 2] and the p-adic result of Jones [9, Theorem 35]; observe that Theorem 3.1 strengthens [3, Lemma 4].

THEOREM 3.1. *Let*

$$L_1(\pi^{s(1)}) \oplus \cdots \oplus L_r(\pi^{s(r)}) \quad \textit{and} \quad K_1(\pi^{t(1)}) \oplus \cdots \oplus K_q(\pi^{t(q)})$$

be two canonical representations of L. *Then* $s(i) = t(i)$, $\dim L_i = \dim K_i$ *and* $N(L_i) \equiv N(K_i) \pmod{\pi^{s(i)+1}}$ *for all* i.

Proof. By considering $N(L)$ we see that $s(1)$ must be equal to $t(1)$. We suffer no loss in generality in assuming that $s(1) = 0 = t(1)$ and consequently that $N(L) \subseteq \mathfrak{o}$. Let (ξ) and (η) be respective canonical bases for L. First we show that $\dim L_i = \dim K_i$ and $s(i) = t(i)$ all i: by defini-

tion of L_i and K_i this is tantamount to proving $\max|\xi_j\cdot Z| = \max|\eta_j\cdot Z|$ all j, $Z\in L$. If not, let ξ_d be the first point of discrepancy: $\max|\xi_d\cdot Z| < \max|\eta_d\cdot Z| = |\pi^\delta|$, say. Then expressing (η_j) in terms of the (ξ_j) we see that

$$\eta_1 = a_{11}\xi_1 + \cdot\cdot\cdot + a_{1d-1}\xi_{d-1} + N_1$$
$$\cdot\;\cdot\;\cdot \qquad \cdot\;\cdot\;\cdot \qquad \cdot\;\cdot\;\cdot$$
$$\eta_d = a_{d1}\xi_1 + \cdot\cdot\cdot + a_{dd-1}\xi_{d-1} + N_d$$

where $\max|N_i\cdot Z| < |\pi^\delta|$ and hence by adding vertically we see that there must exist integers λ_γ with at least one λ_γ a unit such that $\sum^d\lambda_\gamma\cdot\eta_\gamma = \sum^d\lambda_\gamma\cdot N_\gamma$ Now $\max|N_\gamma\cdot Z| < |\pi^\delta|$ and $\max|\eta_\gamma\cdot Z| \geqq |\pi^\delta|$ provided that $\gamma \leqq d$. Since one of the λ_γ is a unit this establishes a contradiction and the first contention is proved.

Suppose now that i is an integer for which $L_i(\pi^t)$ and $K_i(\pi^t)$ are of different *type*: let $K_i = \mathfrak{o}\eta_\mu + \cdot\cdot\cdot$ be proper. Then there is an $N\in L$ with the property that $|N^2| = |\pi^t|$ and $|N\cdot Z| \leqq |\pi^t|$ for all $Z\in L$. We aim to exhibit an M orthogonal to $\xi_1,\cdot\cdot\cdot,\xi_{\mu-1}$ such that $|M^2| = |\pi^t|$. Put $M = (N - \lambda_1\cdot\xi_1\cdot\cdot\cdot - \lambda_{\mu-1}\xi_{\mu-1})$ where λ_j are integers defined for $j<\mu$ in the following way: (1) if $\xi_i\cdot\xi_k = 0$ all $k\neq j$ write $\lambda_j = (N\cdot\xi_j)/\xi_j^2$. Then $|\lambda_j| \leqq |\pi^t|/|\xi_j^2|$ and λ_j is therefore an integer since $j<\mu$. In addition $|(\lambda_j\cdot\xi_j)^2| \leqq |\pi^{2t}|/|\xi_j^2| < |\pi^t|$ since $j<\mu$; and similarly $|2\lambda_j\cdot(N\cdot\xi_j)| \leqq |\pi^{2t}|/|\xi_j^2| < |\pi^t|$. (2) if on the other hand ξ_j is not orthogonal to ξ_{j-1} (say), choose λ_j and λ_{j-1} as the *integral* solutions of the equations

$$N\cdot\xi_j = \lambda_j\cdot\xi_j^2 + \lambda_{j-1}\cdot(\xi_j\cdot\xi_{j-1})$$
$$N\cdot\xi_{j-1} = \lambda_j\cdot(\xi_j\cdot\xi_{j-1}) + \lambda_{j-1}\cdot\xi_{j-1}^2.$$

Then $|\xi_j^2\cdot\xi_{j-1}^2 - (\xi_j\cdot\xi_{j-1})^2| = |(\xi_j\cdot\xi_{j-1})^2|$ since $|\xi_j^2| < |\xi_j\cdot\xi_{j-1}|$ and $|\xi_{j-1}^2| < |\xi_j\cdot\xi_{j-1}|$, (ξ) being a canonical basis; direct computation then shows that $|\lambda_j| \leqq |\pi^t|/|\xi_j\cdot\xi_{j-1}|$ and $|\lambda_{j-1}| \leqq |\pi^t|/|\xi_j\cdot\xi_{j-1}|$, so that λ_j and λ_{j-1} are certainly integers. Multiplication shows that $|(\lambda_j\cdot\xi_j + \lambda_{j-1}\cdot\xi_{j-1})^2| < |\pi^t|$ and $|2N\cdot(\lambda_j\cdot\xi_j + \lambda_{j-1}\cdot\xi_{j-1})| < |\pi^t|$.

The properties proved in (1) and (2) show that $M^2 \equiv N^2 \pmod{\pi^{t+1}}$ and hence $|M^2| = |\pi^t|$. In addition the λ_j in both (1) and (2) were chosen in such a way that $M\cdot\xi_j = 0$ all $j<\mu$. Hence $L_i(\pi^t)$ must represent a number of ordinal t. Consequently $L_i(\pi^t)$ must be proper. This contradiction completes the proof.

Definition 3.1. Let L and K be two lattices having canonical representations

$$L_1(\pi^{s(1)}) \oplus \cdot\cdot\cdot \oplus L_r(\pi^{s(r)}) \text{ and } K_1(\pi^{t(1)}) \oplus \cdot\cdot\cdot \oplus K_r(\pi^{t(r)})$$

respectively, with $s(1) < \cdots < s(r)$ and $t(1) < \cdots < t(r)$. We say that L and K are of the same type if $s(i) = t(i)$, $\dim L_i = \dim K_i$ and L_i and K_i are proper or improper together, where $1 \leqq i \leqq r$. We call $|\pi^{s(r)}| = |\pi^{t(r)}|$ the least divisor of the type and write $s(r) = m(L)$; we call $|\pi^{s(1)}| = |\pi^{t(1)}|$ the greatest divisor of the type and write $s(1) = M(L)$.

4. Lattices of unit determinant. We are now in a position to characterize lattices of unit determinant over fields in which 2 is not ramified. But first let us state some well-known lemmas in a form more suited to our purposes.

LEMMA 4.1. *Let $e > 0$. If ϵ is a unit in F and if X is a vector in L, then the equation $(\alpha \cdot X)^2 \equiv \epsilon X^2 \pmod{\pi X^2}$ always has a solution α.*

Proof. The required α is any solution of $\alpha^2 \equiv \epsilon \pmod{\pi}$; this always exists in virtue of the fact that the residue class field is perfect, [19].

LEMMA 4.2. *If $X^2 \equiv \epsilon X^2 \pmod{4\pi \cdot X^2}$, then there is an $\alpha \in F$ such that $(\alpha \cdot X)^2 = \epsilon \cdot X^2$.*

Proof. $\epsilon \equiv 1 \pmod{4\pi}$ implies that $\alpha^2 = \epsilon$ has a solution α in F by Hensel's lemma [1].

LEMMA 4.3. *Let $L = \mathfrak{o}\xi_1 + \cdots + \mathfrak{o}\xi_n$ and let (η_i) be another basis for V. Then there is minimal basis (ζ_i) for L with the property $\zeta_i \in F \cdot \eta_1 + \cdots + F \cdot \eta_i$.*

Proof. By induction to n. Write $\xi_i = a_{i1} \cdot \eta_1 + \cdots + a_{in} \cdot \eta_n$ and permute the (ξ_i) until $|a_{nn}| = \max |a_{\lambda n}|$. Then L can be written as $\mathfrak{o}\Xi_1 + \cdots + \mathfrak{o}\Xi_{n-1} + \mathfrak{o}\xi_n$ where $\Xi_i = (\xi_i - a_{in}/a_{nn} \cdot \xi_n) \in F \cdot \eta_1 + \cdots + F \cdot \eta_{n-1}$. Induction completes the proof. [See [2], Theorems 1 and 2.]

Now we give the characterization mentioned above.

THEOREM 4.4. *Let L and K be totally integral lattices of unit determinant in the same metric space V. If $N(L) = (2) \cdot \mathfrak{o} = N(K)$ then $L \cong K$. If $e = 1$ and $N(L) = N(K)$ then $L \cong K$.*

Proof. If $N(L)$ and $N(K)$ are both equal to $(2) \cdot \mathfrak{o}$ then L and K are maximal lattices [11] of norm $(2) \cdot \mathfrak{o}$ and hence $L \cong K$ by [11, Sätz 9.6]. This proves the first part of the theorem and from now on we can take $e = 1$. There are two possibilities: (1) if L is proper then $N(L) = \mathfrak{o} = N(K)$ and K is therefore proper too; (2) if L is improper then L contains a vector of norm $(2) \cdot \mathfrak{o}$: for if $\xi_1, \xi_2, \cdots$ denotes a canonical basis for L then $|\xi_1^2|$ or

$|\xi_2^2|$ or $|(\xi_1+\xi_2)^2|$ must be equal to $|2|$; hence $N(L)=(2)\cdot\mathfrak{o}=N(K)$ and this possibility has already been proved. The problem therefore reduces to the case (1) where L and K are both proper: let $L=\mathfrak{o}\xi_1+\cdots+\mathfrak{o}\xi_n$ and $K=\mathfrak{o}\zeta_1+\cdots+\mathfrak{o}\zeta_n$ and proceed by induction to n.

If we assume that either L or K does not represent $\{\pi^2\}$ non-trivially (let us say L) then we can show that L is precisely K as follows: since L and K are in the same space we have $\zeta_j=a_{1j}\cdot\xi_1+\cdots+a_{nj}\cdot\xi_n$ and suppose that $|a_{ij}|=\max|a_{\lambda j}|$ is greater than 1; then $|(a_{ij}^{-1}\cdot\zeta_j)^2|\leqq|\pi^2|$ since $|a_{ij}^{-1}|\leqq|\pi|$ and ζ_j^2 is integral. But $a_{ij}^{-1}\cdot\zeta_j$ is an element of L since its ξ_i coefficient is a unit; its norm is therefore a non-trivial representation of $\{\pi^2\}$ which is impossible. Hence a_{ij} must be integral for all i, j. Hence $K\subseteq L$ and since $|d(L)|=|d(K)|$, L must be equal to K.

We may now assume that both L and K represent $\{\pi^2\}$ non-trivially. First we complete the induction when n is even. Our assumptions guarantee a vector X in L such that $X^2=\{\pi^2\}$ and $X\cdot\xi_1$ (say) equals 1. By Lemma 4.3 we may write $L=\mathfrak{o}\xi_1+\mathfrak{o}(\alpha\cdot X+\beta\cdot\xi_1)+\cdots$; then if $|\alpha|>1$ or if $|\beta|>1$, $|\alpha|=|\beta|$ since $\pi^{-1}\cdot X\notin L$ and $\pi^{-1}\cdot\xi_1\notin L$; now $\alpha\cdot X^2+\beta\cdot(X\cdot\xi_1)\,\varepsilon\,\mathfrak{o}$ and so $|\beta|\leqq 1$; hence $\alpha\,\varepsilon\,\mathfrak{o}$ also; it follows that $L=\mathfrak{o}\xi_1+\mathfrak{o}X+\cdots$ and hence $L=(\mathfrak{o}\xi_1+\mathfrak{o}X)\oplus L_1=L_0\oplus L_1$ in virtue of Lemma 2.2. Then $L_0=\mathfrak{o}\Xi_1+\mathfrak{o}\Xi_2$ with $\Xi_2^2=1+2\beta$, $\beta\,\varepsilon\,\mathfrak{o}$, $\Xi_1^2=\{\pi^2\}$ and $\Xi_1\cdot\Xi_2=1$ in virtue of Lemma 4.1. Then $\Xi_2-\beta\cdot\Xi_1\,\varepsilon\,L_0$ and its norm is equal to $1+\{\pi^2\}$. We now repeat this step and obtain $(\Xi_2-(\beta+\pi\gamma)\cdot\Xi_1)^2=1+\{\pi^3\}$. Hence by Lemma 4.2 L_0 must represent 1. Therefore there is a $Y\,\varepsilon\,L$ and (by symmetry) a $Z\,\varepsilon\,K$ such that $Y^2=1=Z^2$. Then $L=\mathfrak{o}Y\oplus L_2$ and $K=\mathfrak{o}Z\oplus K_2$ in virtue of Lemmas 4.3 and 2.1. Now L_2 and K_2 are in isometric spaces by the Witt cancellation law; they are both proper being of unit determinant and of odd dimension; hence $L_2\cong K_2$; hence $L\cong K$.

Now let n be odd, $n\geqq 3$. Once again it is possible to write $L=L_0\oplus L_1$ with $L_1=\mathfrak{o}\Xi_3\oplus\cdots\oplus\mathfrak{o}\Xi_n$ and $L_0=\mathfrak{o}\Xi_1+\mathfrak{o}\Xi_2$ where $\Xi_1^2=\{\pi^2\}$, $\Xi_1\cdot\Xi_2=1$, $\Xi_2^2=1+\{\pi\}$. If $\Xi_1^2=[\pi^2]$, replace Ξ_1 by $\Xi_1+\gamma\pi\cdot\Xi_3$ in such a way that $(\Xi_1+\gamma\pi\cdot\Xi_3)^2=\{\pi^3\}$ (Lemma 4.1) and write

$$L=(\mathfrak{o}(\Xi_1+\gamma\pi\cdot\Xi_3)+\mathfrak{o}\Xi_2)\oplus L_3$$

by Lemma 2.2. In any case we have $L=L_2\oplus L_3$ and similarly $K=K_2\oplus K_3$ where L_2 and K_2 are proper lattices in 2-dimensional spaces of determinant $-1+\{\pi^3\}$, that is to say of determinant -1. These two spaces are isometric [20] and so $L_2\cong K_2$ since the theorem has already been shown to hold for $n=2$. It follows that L_1 and K_1 are in isometric spaces of odd

dimension, are therefore both proper and hence by the inductive hypothesis are both isometric. Hence $L \cong K$. Q. E. D.

Note 4. 1. This is the first point at which the ramified theory differs essentially from the case where 2 is a prime, for in general it is not true that two totally integral lattices of unit determinant in the same metric space are isometric, even if their norms are the same. However, an answer can be given for this case and we will carry this out after finishing the unramified theory.

Note 4. 2. The restriction that the residue class field be perfect is also an important one and Lemma 4. 1 is fundamental in these discussions. Even if $e = 1$, Theorem 4. 4 need not hold with an imperfect residue class field as the following example will show: let Q be the rational numbers with the 2-adic valuation and extend the valuation to $Q[t]$ by defining $| a_0 + a_1 t + \cdots a_n t^n | = \max | a_\lambda |$ as in [1, p. 26] and then to $Q(t)$ by taking quotients. Let $Q(t)^*$ denote the completion of $Q(t)$. Then $(2t - 1) \cdot x^2 + (2t + 1) \cdot y^2$ and $t \cdot x^2 + (4t^2 - 1)/t \cdot y^2$ are fractionally equivalent but not integrally equivalent over $Q(t)^*$. If $e = 0$, the perfectness of the residue class field is no longer essential: see [3, 4] and Section 6 of this paper. The rational p-adic form of Theorem 4. 4 can be found in [9, Theorem 36].

5. The cancellation law. Examples [3] show that very little indeed can be expected in the way of a cancellation law over a general local field and this is especially true if 2 splits in F. However, the following form will be found useful in the ramified theory:

THEOREM 5. 1. *Let L be a lattice having the two decompositions $L = \mathfrak{o}\xi \oplus L_1$ and $L = \mathfrak{o}\eta \oplus K_1$ with $\xi^2 = \epsilon = \eta^2$ and $|\epsilon| = 1$. Suppose further that $| U \cdot W | \leqq | 2 |$ for all U and W in L_1. Then $L_1 \cong K_1$.*

Proof. Write $\eta = \epsilon_1 \cdot \xi + \pi^\gamma \cdot X$ with X a vector in L_1 having the properties $X \cdot \xi = 0$ and $\pi^{-1} \cdot X \notin L_1$. If $| X^2 | = \max | X \cdot Z |$, $Z \in L_1$, then

$$L = \mathfrak{o}\xi \oplus (\mathfrak{o}X + \textstyle\sum \mathfrak{o}T_\lambda) = \mathfrak{o}\xi \oplus \mathfrak{o}X \oplus \sum \mathfrak{o}T_\lambda' = \mathfrak{o}\eta \oplus \mathfrak{o}X' \oplus \sum \mathfrak{o}T_\lambda'$$

using lemmas 4. 3, 2. 1 and 2. 1 in that order. A determinantal consideration shows that $(X)^2 \cong (X')^2$. But $L_1 = \mathfrak{o}X \oplus \sum \mathfrak{o}T_\lambda'$ and $K_1 = \mathfrak{o}X' \oplus \sum \mathfrak{o}T_\lambda'$ and so $L_1 \cong K_1$.

So assume that $| X^2 | < \max | X \cdot Z |$, $Z \in L_1$, from now on. We will be interested in the number $\pi^{2\gamma} \cdot X^2 = \epsilon(1 - \epsilon_1)(1 + \epsilon_1)$. Either $(1 + \epsilon_1) \notin (2\pi) \cdot \mathfrak{o}$ or $(1 - \epsilon_1) \notin (2\pi) \cdot \mathfrak{o}$: for instance, $1 + \epsilon_1 \in (2\pi) \cdot \mathfrak{o}$ implies $1 - \epsilon_1 = 1 + \epsilon_1$

$-2\epsilon_1 = [2]$. By replacing ξ by $-\xi$ if necessary we can assume that $(1+\epsilon_1) \notin (2\pi)\cdot\mathfrak{o}$, that is $|1+\epsilon_1| \geqq |2|$.

Let $N \in L_1$ be such that $|X\cdot N| = \max |X\cdot Z|$, $Z \in L_1$. Then $|X^2| < |N\cdot X|$ and so X and N are linearly independent. Applying Lemma 4.3 to L_1 permits the expansion $L = \mathfrak{o}\xi \oplus (\mathfrak{o}X + \mathfrak{o}(\alpha\cdot X + \beta\cdot N) + \sum\mathfrak{o}T_\lambda)$. Suppose if possible that $|\beta| > 1$ or $|\alpha| > 1$ or both; then $\pi^{-1}\cdot X \notin L_1$ and $\pi^{-1}\cdot N \notin L_1$ and hence $|\alpha| = |\beta|$; but $|(\alpha\cdot X + \beta\cdot N)\cdot X| = |\beta|\cdot|N\cdot X| \leqq |N\cdot X|$ by choice of N; hence $|\beta| \leqq 1$ and so $|\alpha| \leqq 1$. Therefore we can write $L = \mathfrak{o}\xi \oplus (\mathfrak{o}X + \mathfrak{o}N + \sum\mathfrak{o}T_\lambda)$. Since $|X\cdot N| \geqq |X\cdot T_\lambda|$, it is possible to replace the T_λ by $(T_\lambda - (X\cdot T_\lambda)/(N\cdot X)\cdot N)$ and if we continue to call these new vectors T_λ, it follows that

$$X\cdot T_\lambda = 0 \quad\text{and}\quad \xi\cdot T_\lambda = 0. \tag{5.1}$$

Then $L = \mathfrak{o}\xi + \mathfrak{o}X + \mathfrak{o}N + \sum\mathfrak{o}T_\lambda = \mathfrak{o}\eta + \mathfrak{o}(\epsilon_1^{-1}\cdot X) + \mathfrak{o}N + \sum\mathfrak{o}T_\lambda$ since $\eta = \epsilon_1\xi + \pi^\gamma\cdot X$ and since $\mathfrak{o}X = \mathfrak{o}(\epsilon_1^{-1}\cdot X)$. If we now use Lemma 2.1 to orthogonalize with respect to $\mathfrak{o}\eta$ we obtain

$$L = \mathfrak{o}\eta \oplus (\mathfrak{o}Y + \mathfrak{o}M + \sum\mathfrak{o}T_\lambda) \tag{5.2}$$

where $Y = \epsilon_1^{-1}(X - (X\cdot\eta)\cdot\epsilon^{-1}\cdot\eta)$ and $M = (N - (N\cdot\eta)\cdot\epsilon^{-1}\cdot\eta)$ and direct computation yields the following equalities:

$$\begin{gathered} Y\cdot T_\lambda = 0 = X\cdot T_\lambda;\ Y^2 = X^2;\ M\cdot Y = \epsilon_1\cdot(N\cdot X);\ M\cdot T_\lambda = N\cdot T_\lambda; \\ M^2 = N^2 - \pi^{2\gamma}(N\cdot X)^2\cdot\epsilon^{-1}. \end{gathered} \tag{5.3}$$

Now write $L = \mathfrak{o}\eta \oplus (\mathfrak{o}Y + \mathfrak{o}(M + \psi\cdot Y) + \sum\mathfrak{o}T_\lambda)$ where ψ is defined by

$$\psi = \frac{\pi^{2\gamma}(N\cdot X)}{\epsilon(1+\epsilon_1)}. \tag{5.4}$$

Then ψ is an integer since $|N\cdot X| \leqq |2|$ and $|1+\epsilon_1| \geqq |2|$. Also $(M+\psi Y)^2 = N^2$, $(M+\psi Y)\cdot Y = N\cdot X$ and $(M+\psi Y)\cdot T_\lambda = N\cdot T_\lambda$ is easily shown by using equations (5.3) and (5.4). Also $X^2 = Y^2$, $X\cdot T_\lambda = 0 = Y\cdot T_\lambda$ and $T_\lambda\cdot T_\mu = T_\lambda\cdot T_\mu$. Hence L_1 and K_1 are isometric. Q. E. D.

Remark. Let us examine the previous proof under the following set of circumstances: $e \leqq 1$, L_1 and K_1 are totally integral and of the same type, so that $N(L_1) = N(K_1)$. If $|X^2| = \max|X\cdot Z|$, $Z \in L_1$, the proof goes through. If $|N\cdot X| \leqq |2|$, the proof goes through. So let us consider the remaining possibility which fails since ψ in equation (5.4) need not be integral: $|X^2| < \max|X\cdot Z|$ and $|N\cdot X| > |2|$. Then $|X^2| < 1$ and $|N\cdot X| = 1$ since L_1 is totally integral and F is unramified. The equations

of Lemma 2. 2 are therefore seen to have integral solutions when applied to $\mathfrak{o}X + \mathfrak{o}N + \sum \mathfrak{o}T_\lambda$. Hence $L = \mathfrak{o}\xi \oplus (\mathfrak{o}X + \mathfrak{o}N) \oplus L_2$. Now write $L_2 = L_3(\pi^0) \oplus L_4$ as in equation (2. 1). We have therefore expressed $L = \mathfrak{o}\xi \oplus L_5 \oplus L_4$ where $X \,\varepsilon\, L_5$ and $| U \cdot W | \leqq | 2 |$ all U, W in L_4. Then $\mathfrak{o}\xi \oplus L_5 = \mathfrak{o}\eta + L_5 = \mathfrak{o}\eta \oplus K_5$ in virtue of Lemma 2. 1. An application of the cancellation law for fractional equivalence shows that L_5 and K_5 are in isometric spaces. But they are also totally integral lattices of unit determinant and of the same type since $N(L_1) = N(K_1)$. Theorem 4. 4 says they are isometric. We can therefore prove the following result which has already been established over the rational p-adic integers by Jones and Durfee [3, 7, 9, 10]:

THEOREM 5. 2. *Let $e \leqq 1$. If L is a totally integral lattice having the two decompositions $L = L_0 \oplus L_1 = K_0 \oplus K_1$ in which L_0 and K_0 are isometric and of unit determinant, then L_1 and K_1 are isometric provided that $N(L_1) = N(K_1)$.*

Proof. The case where L_0 and K_0 are proper follows immediately by induction on dim L_0 from the previous remark. So now assume that L_0 and K_0 are both improper. Construct a new metric space $V \oplus F \cdot \zeta$ with $\zeta^2 = 1$. Then $L^* = (\mathfrak{o}\zeta \oplus L_0) \oplus L_1 = (\mathfrak{o}\zeta \oplus K_0) \oplus K_1$ has proper first components and so $L_1 \cong K_1$. Q. E. D.

COROLLARY 5. 2. *If L_0 and K_0 are isometric lattices, but not necessarily of unit determinant, and if the least divisor of L_0 is greater than or equal to the greatest divisor of L_1, and if $N(L_1) = N(K_1)$, then $L_1 \cong K_1$.*

6. The odd case. The theory of equivalence over fields for which $e = 0$ can be made to follow very rapidly at this stage. This has been completely worked out [3] so we merely state the results here. We use the notation of equation (2. 1).

THEOREM 6. 1. *L and K are isometric if and only if they are of the same type and $L_i \cong K_i$ for all i, $1 \leqq i \leqq r$. The latter condition is equivalent to* det $(L_i) \cong$ det (K_i) *over a local field whose residue class field is finite.*

THEOREM 6. 2. *If $L = L_0 \oplus L_1 = K_0 \oplus K_1$, then $L_1 \cong K_1$, provided that $L_0 \cong K_0$.*

7. The space invariants. We are now closer to our goal of obtaining a complete set of invariants under integral equivalence and soon we will appeal for assistance to the known theory of fractional equivalence. In particular

we will assume (using the language of metric spaces) that V and V' are isometric if and only if $n(V) = n(V')$, $d(V) = d(V')$ and $S(V) = S(V')$. The notation is as in [20]: n is the dimension of V, d the determinant of V (but for a square factor) and S the algebra $\prod_{\lambda \leqq \mu} (\xi_\lambda^2, \xi_\mu^2)$ where (ξ_λ) is any orthogonal basis for V. We will show that these invariants apply to local fields with perfect residue class fields of characteristic 2: the proof is not relevant to these discussions on integral equivalence so it is relegated to the appendix.

8. Two cases have to be discussed: (1) 2 is a prime in F; (2) 2 is ramified in F. The second requires a more delicate argument than the first, so we will treat the unramified theory separately; in any case we can say much more about it. But first we make the following remark in order to facilitate working with the S-symbols.

Remark. If F is a local field for which $e \geqq 1$, then $(1 + 4\alpha, \epsilon) = 1$ if ϵ is a unit and $\alpha \varepsilon \mathfrak{o}$. Also $(1 + 4\alpha, \epsilon\pi) = 1$ if and only if $1 + 4\alpha$ is a square in F.

Proof. The first part follows immediately if we note that $(1 + 4\alpha)x^2 + \epsilon y^2$ always represents 1. The second follows if we observe that $(1 + 4\alpha)x^2 + \epsilon\pi y^2$ does not represent 1 unless $(1 + 4\alpha)$ is a square.

II. The Unramified Theory.

Throughout this chapter we will assume that $|\pi| = |2|$.

9. Continuous lattices. Let us consider the canonical form $L = L_1(\pi^{s(1)}) \oplus \cdots \oplus L_r(\pi^{s(r)})$ obtained in equation (2.1). We saw in Section 6 that over certain local fields the L_i are independent in the following sense: if $K_1(\pi^{s(1)}) \oplus \cdots \oplus K_r(\pi^{s(r)})$ is another canonical form for L, then $L_i(\pi^{s(i)}) \cong K_i(\pi^{s(i)})$. This is not the case when $|2| < 1$ unless the differences $s(i+1) - s(i)$ are large enough; otherwise the L_i become interwoven and we shall then have to study larger blocks than the mere L_i. To this end we make the following definition:

Definition 9.1. L is said to be a continuous lattice if: (a) $s(i+1) = s(i) + 1$, for all i satisfying $1 \leqq i \leqq r - 1$; (b) the L_i are proper for all $2 \leqq i \leqq r$; (c) L_1 is either proper or improper. If L_1 is proper we say that L is entirely proper.

This notion is well-defined by Theorem 3.1.

THEOREM 9.1. *If L and K are entirely proper continuous lattices in V and if they are both of the same type, then $L \cong K$.*

Proof. We can take $\pi^{s(1)} = \pi^0$ and we can assume that $r > 1$ by Theorem 4.4. First let $n = 2$. Then there is an X in L such that $X^2 = 1 + \lambda\pi$, $\lambda \varepsilon \mathfrak{o}$, in virtue of Lemma 4.1. We want an X with $\lambda \varepsilon (\pi) \cdot \mathfrak{o}$. To that end assume that the λ found above is a unit and let Y be orthogonal to X and such that $Y^2 = \lambda\pi + \{\pi^2\}$; by Lemma 4.1 such a Y must exist. Then $(X + Y)^2 = 1 + \{\pi^2\}$. We can repeat the argument for K. Then $L = \mathfrak{o}Z_1 \oplus \mathfrak{o}Z_2$ and $K = \mathfrak{o}U_1 \oplus \mathfrak{o}U_2$ with $Z_1{}^2 = 1 + \alpha\pi^2$ and $U_1{}^2 = 1 + \beta\pi^2$, both α and β being in $\mathfrak{o}$. Apply the S-symbols to L:

$$S(L) \sim (1 + \alpha\pi^2, -d(L)) \cdot (d(L), d(L)).$$

Then $1 \sim S(L) \cdot S(K) \sim ((1 + \alpha\pi^2)(1 + \beta\pi^2), -d(L))$. Now $|-d(L)| = |\pi|$, hence $(1 + \alpha\pi^2)^{\frac{1}{2}} \cdot (1 + \beta\pi^2)^{\frac{1}{2}} \varepsilon F$ by the remark of Section 8. Hence $(1 + \alpha\pi^2) \cong (1 + \beta\pi^2)$ and therefore $L \cong K$.

For $n > 2$ it is convenient to separate the following two cases:

Case 1. $r = 2$, $\dim L_1 = 1$: Then $\dim L_2 > 1$. Write $L = \mathfrak{o}\xi_1 \oplus (\mathfrak{o}\xi_2 \oplus \cdots \oplus \mathfrak{o}\xi_n)$ with $\xi_2{}^2 = \pi(1 + \{\pi\})$ and then replace ξ_2 by $\Xi_2 = \xi_2 + \alpha\pi \cdot \xi_1$ in such a way that $\Xi_2{}^2 = \pi(1 + \{\pi^2\})$: that this is possible follows from Lemma 4.1. Now replace ξ_1 by $\Xi_1 = (\xi_1 - (\xi_1 \cdot \Xi_2) \cdot (\Xi_2{}^2)^{-1} \cdot \Xi_2)$; then $L = \mathfrak{o}\Xi_1 \oplus \mathfrak{o}\Xi_2 \oplus \mathfrak{o}\xi_3 \oplus \cdots \oplus \mathfrak{o}\xi_n$ since $(\xi_1 \cdot \Xi_2) \cdot (\Xi_2{}^2)^{-1} \varepsilon \mathfrak{o}$. Applying Lemma 4.1 again, we see that Ξ_2 can be replaced by $\Xi_2 + \beta\pi\xi_3$ so that $(\Xi_2 + \beta\pi\xi_3)^2 = \pi(1 + \{\pi^3\})$. Then in virtue of Lemmas 4.2 and 2.1 we see that $L = \mathfrak{o}X \oplus L_1$ with $X^2 = \pi$ and similarly $K = \mathfrak{o}Y \oplus K_1$ with $Y^2 = \pi$. Then L_1 and K_1 are still entirely proper and so $L_1 \cong K_1$ by induction and hence $L \cong K$.

Case 2. $r \geqq 3$ or $\dim L_1 > 1$: As in the case $n = 2$ we can write $L = \mathfrak{o}Z_1 \oplus \cdots \oplus \mathfrak{o}Z_n$ with $Z_1{}^2 = 1 + \{\pi^2\}$. Since $r \geqq 3$ or $\dim L_1 > 1$, there is a Z_i $(i \geqq 2)$ such that $(Z_1 + \alpha Z_i)^2 = 1 + \{\pi^3\}$ with $|\alpha| = 1$ or $|\alpha| = |\pi|$. We can therefore write $L = \mathfrak{o}(Z_1 + \alpha Z_i) \oplus L_1$ in virtue of Lemma 2.1, where L_1 is still entirely proper; and using Lemma 4.2, $L = \mathfrak{o}Z \oplus L_1$ with $Z^2 = 1$. And similarly $K = \mathfrak{o}W \oplus K_1$ with $W^2 = 1 = Z^2$ and K_1 entirely proper. Then L_1 and K_1 are in isometric spaces of dimension $n - 1$; by induction $L_1 \cong K_1$; hence $L \cong K$. Having considered all possible cases, the proof is now through.

THEOREM 9.2. *Any two continuous lattices of the same type and in the same metric space V are isometric.*

Proof. Again take $\pi^{s(1)} = \pi^0$ and use induction to n. We may take $r > 1$ by Theorem 4. 4. Express L in a canonical basis: $L = (\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2) \oplus L_1$. If $F \cdot \xi_1 + F \cdot \xi_2$ represents 0 non-trivially, do not proceed further. If not, then $\xi_1{}^2 = \alpha\pi$, α being a unit. Since $r > 1$, we can choose an X orthogonal to ξ_1 in such a way that $X^2 = \alpha\pi + \{\pi^2\}$ in virtue of Lemma 4. 1. Then write $L = (\mathfrak{o}(\xi_1 + X) + \mathfrak{o}\xi_2) \oplus L_2 = L_0 \oplus L_2$, which can be done by Lemma 2. 2. Moreover L_0 represents zero non-trivially since $d(L_0) \cong -1$. Similarly for $K = K_0 \oplus K_2$. Then $L_0 \cong K_0$ by Theorem 4. 4. So L_2 and K_2 are in isometric spaces and hence $L_2 \cong K_2$. Therefore $L \cong K$.

10. Congruence of lattices. Let us prove some fundamental lemmas which we will need in the next section. By an i-dimensional lattice in V we mean a subset of V that is a lattice in some i-dimensional subspace of V.

Definition 10. 1. If L and K are two i-dimensional lattices of V, we say that $L \cong K \pmod{\pi^\omega}$ if there is a transformation A such that $AV = V$, $AL = K$ and $AX \cdot AY \equiv X \cdot Y \pmod{\pi^\omega}$ for all X and Y in L.

We will not need this definition until much later. We mention it here because of the analogy between it and the sharper conditions (2) of the next two lemmas.

Now let L have the matrix $\begin{pmatrix} \{\pi\} & 1 \\ 1 & \{\pi\} \end{pmatrix}$. Then by simple changes of basis and using Lemma 4. 1 we have $L \cong \begin{pmatrix} [\pi] & 1 \\ 1 & \{\pi\} \end{pmatrix} \cong \begin{pmatrix} \pi + \{\pi^2\} & 1 \\ 1 & \alpha\pi \end{pmatrix}$ with $\alpha \varepsilon \mathfrak{o}$. Put $J \cong \begin{pmatrix} \pi & 1 \\ 1 & \alpha\pi \end{pmatrix}$. Contention: $L \cong J$. For if $\alpha \varepsilon (\pi) \cdot \mathfrak{o}$ then L and J are in spaces of determinant (-1), hence in isometric spaces and hence $L \cong J$ by Theorem 4. 4. So now assume that α is a unit. Then $d(L) \cong d(K)$. Also $S(L) \sim (\alpha\pi, \alpha\pi) \cdot (\alpha\pi \cdot d(L), d(L)) \sim S(J)$. Hence L and K are in isometric spaces and so once again $L \cong J$.

LEMMA 10. 1. *If L and K are two i-dimensional lattices of V, both having the same least divisor $|\pi^m|$, and if there is a transformation A of V onto itself with the properties*: (1) $AL = K$; (2) *if X and $Y \varepsilon L$, then* $AX \cdot AY \equiv X \cdot Y \pmod{\pi^{m+1}}$ *and* $(AX)^2 \equiv X^2 \pmod{\pi^{m+2}}$; (3) $d(L) \cong d(K)$; *then L is isometric to K.*

Proof. By induction to i. We use the notation of equation (2. 1). There is no loss in generality if we assume that $s(1) = 0$ for L and that both L and K are totally integral. If $i = 1$ there is nothing to prove. If $i = 2$ and L is improper, then $L \cong \begin{pmatrix} \pi & 1 \\ 1 & \alpha\pi \end{pmatrix}$ by the contention proved

above and so $K \cong \begin{pmatrix} \pi + \{\pi^2\} & 1 + \{\pi\} \\ 1 + \{\pi\} & \alpha\pi + \{\pi^2\} \end{pmatrix} \cong \begin{pmatrix} \pi + \{\pi^2\} & 1 \\ 1 & \alpha\pi + \{\pi^2\} \end{pmatrix}$. If $\alpha \varepsilon (\pi) \cdot \mathfrak{o}$, then $d(L) \cong -1 \cong d(K)$ and Theorem 4.4 carries us through. If $|\alpha| = 1$, the result follows from the contention proved above.

We can now start the induction for general i, but distinguishing the three cases:

Case 1. $r = 1$ and $L_1(\pi^{s(1)})$ is proper: Write $L = \mathfrak{o}\xi_1 \oplus \cdots \oplus \mathfrak{o}\xi_i = \mathfrak{o}\xi_1 \oplus L_2$ and then $K = \mathfrak{o}(A\xi_1) + \cdots + \mathfrak{o}(A\xi_i) = \mathfrak{o}\eta_1 \oplus (\mathfrak{o}\eta_2 + \cdots + \mathfrak{o}\eta_i) = \mathfrak{o}\eta_1 \oplus K_2$, where $\eta_1 = A\xi_1$ and $\eta_j = A\xi_j - (A\xi_1 \cdot A\xi_j) \cdot ((A\xi_1)^2)^{-1} \cdot A\xi_1$ for $2 \leqq j \leqq i$. Then it is easy to see that $\eta_j{}^2 \equiv \xi_j{}^2 \pmod{\pi^2}$ and that $\xi_j \cdot \xi_h \equiv \eta_j \cdot \eta_h \pmod{\pi}$. Now write $K = \mathfrak{o}(\eta_1 + \alpha\pi \cdot \eta_2) + \mathfrak{o}\eta_2 + \cdots + \mathfrak{o}\eta_i$ with α chosen so that $(\eta_1 + \alpha\pi \cdot \eta_2)^2 \cong \xi_1{}^2$: this can be done in virtue of Lemmas 4.1 and 4.2, observing that $\eta_1{}^2 = (A\xi_1)^2 \equiv (\xi_1{}^2) \pmod{\pi^2}$. Now use Lemma 2.1 to write $K = \mathfrak{o}(\eta_1 + \alpha\pi \cdot \eta_2) \oplus K_2{}^*$. Then $K_2{}^*$ and L_2 have the properties enunciated in the statement of the lemma, hence $L_2 \cong K_2{}^*$ and so $L \cong K$.

Case 2. $r \geqq 1$, $L_1(\pi^{s(1)})$ improper: Express L canonically:

$$L = (\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2) \oplus (\mathfrak{o}\xi_3 + \cdots + \mathfrak{o}\xi_i) = L_0 \oplus L_1.$$

Then it is possible to write

$$K = (\mathfrak{o}(A\xi_1) + \mathfrak{o}(A\xi_2)) \oplus (\Sigma\mathfrak{o}(A\xi_\lambda + \alpha_\lambda(A\xi_1) + \beta_\lambda(A\xi_2))) = K_0 \oplus K_1$$

where α_λ and β_λ are determined by Lemma 2.2 and are therefore in $(\pi^{m+1}) \cdot \mathfrak{o}$. Then $L_0 \cong K_0$ and we can apply induction to L_1 and K_1 to obtain $L \cong K$.

Case 3. $r > 1$, $L_1(\pi^{s(1)})$ proper: This is almost the same as Case 1, except that $m > 0$. We get $K = \mathfrak{o}\eta_1 \oplus K_2$ as before. Then $\eta_1{}^2 \equiv \xi_1{}^2 \pmod{\pi^3}$, hence $\eta_1{}^2 \cong \xi_1{}^2$, hence $L \cong K$. Q. E. D.

Definition 10.2. If $L_1(\pi^{s(1)}) \oplus \cdots \oplus L_r(\pi^{s(1)})$ is a canonical form for L, we say that L is a proper lattice if $L_r(\pi^{s(r)})$ is proper; we say that L is improper if $L_r(\pi^{s(r)})$ is improper.

The reason for this strange definition will become apparent in the next two sections.

LEMMA 10.2. *If L and K are two i-dimensional lattices in V, both having the same least divisor $|\pi^m|$, and if there is a transformation A of V onto itself with the properties:* (1) $AL = K$; (2) $AX \cdot AY \equiv X \cdot Y \pmod{\pi^\omega}$ *and* $(AX)^2 \equiv X^2 \pmod{\pi^{\omega+1}}$ *for all X and Y in L, where $\omega = m + 1$ if L is improper and $\omega = m + 2$ if L is proper, then L and K are isometric.*

Proof. An inductive argument yields $d(L) \cong d(K)$. Now apply Lemma 10.1. Q. E. D.

11. Discontinuous decompositions. In Section 9 we pointed out that the $L_i(\pi^{s(i)})$ would be too small for our purposes and we accordingly introduced larger blocks which we called continuous lattices. It is clear how to subdivide a lattice $L = L_1(\pi^{s(1)}) \oplus \cdots \oplus L_r(\pi^{s(r)})$ into continuous lattices of maximal dimension. Let us write the subdivision $L = M(1) \oplus \cdots \oplus M(q)$. If $L = M'(1) \oplus \cdots \oplus M'(q)$ is another such decomposition, it is clear that $M(i)$ will have the same type as $M'(i)$, but it is still not true that $M(i)$ must be isometric to $M'(i)$. However, it will not be difficult to show how the $M(i)$ change when we pass to the $M'(i)$. To that end we make the following definition:

Definition 11. 1. Consider the decomposition $L = K \oplus J$. We say that this decomposition is discontinuous if either (1) K is improper and $(\pi^{m(K)+2}) \cdot \mathfrak{o} \supseteq N(J)$ or (2) K is proper and $(\pi^{m(K)+3}) \cdot \mathfrak{o} \supseteq N(J)$. We call the decomposition semicontinuous if (3) K is proper and $(\pi^{m(K+2)}) \cdot \mathfrak{o} = N(J)$. The notation is an in Definitions 3. 1 and 10. 2.

LEMMA 11. 1. *Let L and K be two lattices with discontinuous decompositions $L = L(1) \oplus L(2)$ and $K = K(1) \oplus K(2)$ such that $L(1)$ and $K(1)$ have the same type. Then $L \cong K$ if and only if $L(1) \cong K(1)$ and $L(2) \cong K(2)$.*

Proof. The sufficiency is clearly true. To prove the necessity we can assume that $L = K$ and then

$$L = L(1) \oplus L(2) = (\mathfrak{o}\xi_1 + \cdots + \mathfrak{o}\xi_i) \oplus (\mathfrak{o}\xi_{i+1} + \cdots + \mathfrak{o}\xi_n)$$

$$L = K(1) \oplus K(2) = (\mathfrak{o}\eta_1 + \cdots + \mathfrak{o}\eta_i) \oplus (\mathfrak{o}\eta_{i+1} + \cdots + \mathfrak{o}\eta_n)$$

in the canonical bases (ξ) and (η). Then

$$\begin{aligned} \eta_1 &= a_{11}\xi_1 + \cdots + a_{i1}\xi_i + N_1 = \Xi_1 + N_1 \\ &\cdots \qquad \cdots \qquad \cdots \qquad \cdots \\ \eta_i &= a_{1i}\xi_1 + \cdots + a_{ii}\xi_i + N_i = \Xi_i + N_i \end{aligned} \tag{11. 1}$$

where $a_{ij} \in \mathfrak{o}$ since $\eta_j \in L$. Also $| N_j^2 | \leqq | \pi^{\omega+1} |$ by Definition 11. 1 and similarly $| N_j \cdot Z | \leqq | \pi^{\omega} |$ all $Z \in L$, ω being $m(L(1)) + 1$ or $m(L(1)) + 2$, depending on whether $L(1)$ is improper or proper.

Now it is clear from equation (11. 1) that $| \det(\mathfrak{o}\Xi_1 + \cdots + \mathfrak{o}\Xi_i) | = | \det(K(1)) | = | \det(L(1)) |$. Hence $\mathfrak{o}\Xi_1 + \cdots + \mathfrak{o}\Xi_i = L(1)$. Define $A\Xi_j = \eta_j$ for all $j \leqq i$ and extend it to a transformation of V onto V. Then $\eta_j^2 \equiv \Xi_j^2 \pmod{\pi^{\omega+1}}$ and $\eta_j \cdot \eta_h \equiv \Xi_j \cdot \Xi_h \pmod{\pi^{\omega}}$; hence $(AX)^2 \equiv X^2 \pmod{\pi^{\omega+1}}$ and $AX \cdot AY \equiv X \cdot Y \pmod{\pi^{\omega}}$ for all X and Y in $L(1)$. The

conditions of Lemma 10. 2 are satisfied and so $L(1) \cong K(1)$. Applying Corollary 5. 2 yields $L(2) \cong K(2)$ and the lemma is proved.

LEMMA 11. 2. *Let the lattice L have two semi-continuous decompositions* $L = L(1) \oplus L(2)$ *and* $L = K(1) \oplus K(2)$. *Then* $d(L(1))/d(K(1)) \cong 1 \pmod{\pi^2}$ *and*

$$(d(L(1)), \pi^{\operatorname{ord} d(L(1))+m(L(1))}) \cdot S(L(1))$$
$$\sim (d(K(1)), \pi^{\operatorname{ord} d(K(1))+m(K(1))}) \cdot S(K(1))$$

provided that $L(1)$ *and* $K(1)$ *are both of the same type.*

Proof. We obtain the system of equations (11. 1) in the same way as before. Then $a_{ij} \varepsilon \mathfrak{o}$ and $|N_j^2| \leqq |\pi^{m+2}|$ and similarly $|N_j \cdot Z| \leqq |\pi^{m+1}|$ all Z in L. Once again $L(1) = \mathfrak{o}\Xi_1 + \cdots + \mathfrak{o}\Xi_i$. In addition it is easy to see that $d(L(1))/d(K(1)) \cong 1 \pmod{\pi^2}$ by considering the determinant of $(\Xi_\lambda \cdot \Xi_\mu)$ where $\Xi_\lambda = \eta_\lambda - N_\lambda$.

Now suppose for the moment that $d(L(1)) \cong d(K(1))$. Define $A\Xi_j = \eta_j$ for $j \leqq i$ and extend it to V. The conditions of Lemma 10. 1 are satisfied and so $L(1) \cong K(1)$, hence

$$S(L(1)) \sim S(K(1)) \tag{11.2}$$

and hence the lemma is true.

If on the other hand $d(L(1))/d(K(1)) = a^2 + \epsilon\pi^2$, ϵ being a unit, it is possible to write

$$L = (\mathfrak{o}\xi_1 + \cdots + \mathfrak{o}\xi_{i-1} + \mathfrak{o}(\xi_i + \alpha\xi_{i+1})) \oplus L(2)^* = L(1)^* \oplus L(2)^*, \tag{11.3}$$

$\alpha \varepsilon \mathfrak{o}$, where ξ_{i+1} has norm $|\xi_{i+1}^2| = |\pi^{m+2}|$ in virtue of Lemma 2. 1. Now ξ_i and therefore $(\xi_i + \alpha\xi_{i+1})$ is orthogonal to all the remaining $\xi_1, \cdots, \xi_{i-1}$ since the original decomposition was semi-continuous. Hence, with the aid of Lemma 4. 1, an $\alpha \varepsilon \mathfrak{o}$ can be chosen in such a way that $d(L(1)^*)/d(K(1)) = a^2 + \{\pi^3\}$ and therefore $d(L(1)^*) \cong d(K(1))$.

Referring to equation (11. 2) we see that

$$S(L(1)) \cdot S(K(1)) \sim S(L(1)) \cdot S(L(1)^*).$$

Direct computation shows that

$$S(L(1)) \cdot S(L(1)^*) \sim (-d(\mathfrak{o}\xi_1 + \cdots + \mathfrak{o}\xi_{i-1}), d(L(1)^*) \cdot d(L(1)))$$

and this is the same as

$$(\pi^{\operatorname{ord} d(L(1))+m(L(1))}, d(L(1)) \cdot d(K(1)))$$

since

$$d(L(1))d(L(1)^*) \cong d(L(1))d(K(1)) \cong 1 + \{\pi^2\},$$

in virtue of the remark of Section 8. Hence the second part of the lemma is generally true.

12. Complete set of invariants. We now have enough available to be able to tell whether two lattices are isometric or not and we tie these results together in the form of a complete set of invariants. We will work with the decomposition $L = M(1) \oplus \cdots \oplus M(q)$ given in Section 11. Let K be another lattice in V having the same type as L and with the decomposition $K = P(1) \oplus \cdots \oplus P(q)$.

If we consider the decomposition $L = L(1) \oplus L(2)$ where

$$L(1) = M(1) \oplus \cdots \oplus M(j) \text{ and } L(2) = M(j+1) \oplus \cdots \oplus M(q),$$

then it is easy to see that this decomposition is either discontinuous or else semi-continuous. Hence, if $L \cong K$ it follows from Lemmas 11.1 and 11.2 that

$$\frac{d(M(1) + \cdots + M(j))}{d(P(1) + \cdots + P(j))} \cong 1 \ (\mathrm{mod}\ \pi^{\gamma(j)}) \tag{12.1}$$

holds for any j, $1 \leqq j \leqq q$, $\gamma(j)$ being 2 or 3 depending on whether the break from j to $j+1$ is semi-continuous or discontinuous. In addition

$$(d(M(1) + \cdots + M(j)), \pi^{\mathrm{ord}\, d(M(1)+\cdots+M(j))+m(j)}) \cdot S(M(1) + \cdots + M(j)) \tag{12.2}$$

is the same for both lattices, if $m(j)$ denotes the ordinal of the least divisor of $M(j)$.

We now show that the converse is true by using induction to q. Let

$$M = M(1) \oplus \cdots \oplus M(q-1) = \mathfrak{o}\xi_1 + \cdots + \mathfrak{o}\xi_i$$

and let

$$P = P(1) \oplus \cdots \oplus P(q-1) = \mathfrak{o}\eta_1 + \cdots + \mathfrak{o}\eta_i,$$

the bases being canonical. If the break from $q-1$ to q is discontinuous, then $d(P) \cong d(M)$ and $S(P) \sim S(M)$ and hence, by the induction, $P \cong M$. Then $P(q)$ and $M(q)$ are continuous lattices in isometric spaces and hence isometric by Theorem 9.2. Hence $L \cong K$.

If, however, the break from $q-1$ to q is semi-continuous, we must proceed with a little more caution. Exactly as in equation (11.3) we can change ξ_i into $\xi_i + \alpha\xi_{i+1}$ so that L now appears as

$$L = M(1) \oplus \cdots \oplus M(q-2) \oplus M(q-1)^* \oplus M(q)^* = M^* \oplus M(q)^*$$

in such a way that $d(M^*) \cong d(P)$. Then direct computation yields

$S(M) \cdot S(M^*) \sim S(M) \cdot S(P)$ and hence $M^* \cong P$, by the induction. Then $M(q)^* \cong P(q)$, being continuous lattices in isometric spaces. Hence $L \cong K$.

We can therefore formulate the invariants in

THEOREM 12.1. *A complete set of invariants for L is given by*

(1) *the type of L*

(2) $\left(\dfrac{d(M(1)+\cdots+M(j))}{\pi^{\operatorname{ord} d(M(1)+\cdots+M(j))+\gamma(j)}}\right)$

(3) $(\pi^{\operatorname{ord} d(M(1)+\cdots+M(j))+m(j)}, d(M(1)+\cdots+M(j))) \cdot S(M(1)+\cdots+M(j))$

for all j, $1 \leqq j \leqq q$, $\gamma(j)$ being 2 at a semi-continuity and 3 at a discontinuity.

III. The Ramified Theory.

13. We now discuss the ramified case and we aim to show that two totally integral lattices L and K of unit determinant and in the same metric space V are isometric, provided that they represent the same numbers. The main difficulty will be in the case of improper lattices and our plan is to settle (1) the 2-dimensional case (2) the 4-dimensional improper case (3) the general improper case (4) the general case.

We observe that the problem is already solved in Theorem 4.4 whenever $N(L) = (2) \cdot \mathfrak{o}$ and we accordingly introduce this notation: ν will denote the integer defined by $N(L) = (\pi^\nu) \cdot \mathfrak{o}$ and we will assume that $\nu < e$; unless otherwise stated we will make the further assumption that $0 < \nu < e$.

14. Two-dimensional lattices. Throughout this section L and K will stand for improper 2-dimensional lattices of unit determinant with norm π^ν where $0 < \nu < e$. We shall show how to reduce such lattices to a certain standard form.

LEMMA 14.1. *Let $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ be an improper lattice of unit determinant such that $|\xi_1{}^2| = |\pi^\nu|$ and $\xi_1 \cdot \xi_2 = 1$. Then there is an X in L such that $L = \mathfrak{o}\xi_1 + \mathfrak{o}X$, $\xi_1 \cdot X = 1$ and $X^2 = [\pi^\mu]$ where μ ($> \nu$) is such that either $\mu \geqq 2e - \nu$ or else $\mu + \nu$ is odd.*

Proof. Express $L = \mathfrak{o}\xi_1 + \mathfrak{o}Y$ with $\xi_1 \cdot Y = 1$ and such that $|Y^2|$ is least for all such Y. If $\operatorname{ord} Y^2 \geqq 2e - \nu$ or $\operatorname{ord} Y^2 + \nu$ is odd, we are through. So assume that $\operatorname{ord} Y^2 < 2e - \nu$ and that $\operatorname{ord} Y^2 + \nu$ is even. In virtue of Lemma 4.1 there is a unit α such that

$$(\alpha\pi^r\xi_1)^2 \equiv Y^2 \pmod{\pi Y^2} \tag{14.1}$$

where $r = \frac{1}{2}(\operatorname{ord} Y^2 - \nu)$ and $\alpha\pi^r$ is of course integral. Put $X = Y + \alpha\pi^r\xi_1$ and then $L = \mathfrak{o}\xi_1 + \mathfrak{o}X$. Then $|X^2| = |Y^2 + \alpha^2\pi^{2r}\xi_1{}^2 + 2\alpha\pi^r\xi_1 \cdot Y| < |Y^2|$ by equation (14.1) and since $|2\alpha\pi^r\xi_1 \cdot Y| < |Y^2|$. Also $\xi_1 \cdot X = \delta$ is a unit. Hence $L = \mathfrak{o}\xi_1 + \mathfrak{o}(\delta^{-1}X)$ has the properties $\xi_1 \cdot (\delta^{-1}X) = 1$ and $|(\delta^{-1}X)^2| < |Y^2|$. This denies the minimality of $|Y^2|$ and therefore proves the theorem. Q. E. D.

Remark 14.1. If the μ of Lemma 14.1 which corresponds to the lattice L is such that $\mu < 2e - \nu$ and if K is another lattice with $d(K) \cong d(L)$ (mod 4) and $N(L) = N(K)$, then the $\mu(K)$ corresponding to K is equal to μ.

Proof. Let us assume that $\mu(K) > \mu$ if possible. Then $d(L)/d(K) = 1 + [\pi^{\mu+\nu}]$ is a square (mod 4) and so $1 + [\pi^{\mu+\nu}] \equiv (1 + \epsilon_1\pi + \epsilon_2\pi^2 + \cdots)^2$ (mod 4); direct expansion shows that this is impossible if $\nu + \mu$ is odd and less than $2e$. Q. E. D.

Notation. Let c's denote fixed representatives in $\mathfrak{o}$ of the residue class field $\mathfrak{o}/(\pi)\cdot\mathfrak{o}$ with the convention that 0 shall be the representative of the zero residue class: thus $c' \equiv c''$ (mod π) if and only if $c' = c''$.

LEMMA 14.2. *If $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ with $|\xi_1{}^2| = |\pi^\nu|$, then there is an X in L such that $L = \mathfrak{o}\xi_1 + \mathfrak{o}X$, $\xi_1 \cdot X = 1$ and*

$$X^2 = (c_0 + c_2\pi^2 + \cdots + c_{2k}\pi^{2k})\pi^\mu + \{\pi^{2e-\nu}\}$$

where $2k + \mu + 1 = 2e - \nu$.

Proof. There is nothing to prove if $\mu \geqq 2e - \nu$; so assume that $\mu < 2e - \nu$. Suppose that we have achieved $c_1 = c_3 = c_5 = \cdots = c_{2i-1} = 0$ when L is written in the form

$$\mathfrak{o}\xi_1 + \mathfrak{o}Y \colon Y^2 = (c_0 + c_2\pi^2 + \cdots + c_{2i}\pi^{2i} + d\pi^{2i+1})\pi^\mu;\ \xi_1 \cdot Y = 1.$$

We aim to find a U such that $L = \mathfrak{o}\xi_1 + \mathfrak{o}U$, $U \cdot Y = 1$ and

$$U^2 = (c_0 + c_2\pi^2 + \cdots + c_{2i}\pi^{2i} + c_{2i+2}\pi^{2i+2} + \{\pi^{2i+3}\})\pi^\mu \tag{14.2}$$

provided that $2i + \mu + 1 < 2e - \nu$.

If $d \in (\pi)\cdot\mathfrak{o}$ we are through. If not, there is a unit α such that $(\alpha\pi^r\xi_1)^2 \equiv d\pi^{2i+\mu+1}$ (mod $\pi^{2i+\mu+2}$) where $r = \frac{1}{2}(2i + \mu + 1 - \nu)$ in virtue of Lemma 4.1. Put $L = \mathfrak{o}\xi_1 + \mathfrak{o}Z$ where $Z = Y + \alpha\pi^r\xi_1$. We contend that

$$Z^2 = (c_0 + c_2\pi^2 + \cdots + c_{2i}\pi^{2i} + \{\pi^{2i+2}\})\pi^\mu. \tag{14.3}$$

We have $Y^2 + \alpha^2\pi^{2r}\xi_1{}^2$ equal to the right hand side of equation (14.3) by choice of $\alpha\pi^r$; in addition $2i + \mu + 1 < 2e - \nu$ implies that

$$e + r > 2i + \mu + 1 \tag{14.4}$$

by definition of r; and so $2\alpha\pi^r\xi_1 \cdot Y \varepsilon (\pi^{2i+\mu+2}) \cdot \mathfrak{o}$. Hence equation (14.3) holds.

Now write $U = Z/(\xi_1 \cdot Z)$ and $L = \mathfrak{o}\xi_1 + \mathfrak{o}U$. Then $\xi_1 \cdot U = 1$. In addition, equation (14.2) is satisfied: for

$$U^2 = Z^2(1 + \{\pi^{\nu+r}\})^2 = Z^2(1 + \{\pi^{2\nu+2r}\} + \{\pi^{\nu+r+e}\})$$

and $2\nu + 2r \geqq 2i + \mu + 2$ and $\nu + r + e \geqq 2i + \mu + 2$, by equation (14.4).

We have therefore shown how to pass from Y to U. If we repeat this process sufficiently often we arrive at the X mentioned in the statement of the lemma. Q. E. D.

THEOREM 14.3. *Let L and K be two 2-dimensional lattices such that $N(L) = (\pi^\nu) \cdot \mathfrak{o} = N(K)$. If there is an X in L and a Y in K such that $X^2 = \epsilon\pi^\nu = Y^2$ and if in addition $d(L) \cong d(K)$, then L is isometric to K. The result also holds when $e = \nu$.*

Proof. Applying the invariants of Section 7 we see that L and K can be taken in the same metric space V. If $\nu = e$ an easy computation shows that L and K are maximal [11, p. 50], and the theorem follows from [11, Satz 9.6]. So we can assume that $\nu < e$. In virtue of Lemmas 4.3, 14.1 and 14.2 we can write $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ where $\xi_1{}^2 = \epsilon\pi^\nu$, $\xi_1 \cdot \xi_2 = 1$ and $\xi_2{}^2 = (c_0 + c_2\pi^2 + \cdots + c_{2k}\pi^{2k})\pi^\mu + \alpha(\pi^{2e-\nu})$. In virtue of Lemmas 4.3, 14.1, 14.2 and the Remark 14.1 we can write $K = \mathfrak{o}\eta_1 + \mathfrak{o}\eta_2$ where $\eta_1{}^2 = \epsilon\pi^\nu$, $\eta_1 \cdot \eta_2 = 1$ and $\eta_2{}^2 = (d_0 + d_2\pi^2 + \cdots + d_{2k}\pi^{2k})\pi^\mu + \beta(\pi^{2e-\nu})$. Contention: $d_{2i} = c_{2i}$ all i. If not, let j be the smallest integer for which $d_{2j} \neq c_{2j}$: then $| d_{2j} - c_{2j} | = 1$. Since the determinants differ by a square factor we have

$$\begin{aligned}(-1 + \delta\pi^{\nu+\mu} &+ \epsilon d_{2j}\pi^{\nu+\mu+2j}) \\ &\equiv (-1 + \delta\pi^{\nu+\mu} + \epsilon c_{2j}\pi^{\nu+\mu+2j}) \cdot (1 + A\pi)^2 \qquad (\mathrm{mod}\ \pi^{\nu+\mu+2j+1}).\end{aligned}$$

Hence

$$| \pi^{\nu+\mu+2j} | = | (d_{2j} - c_{2j})\pi^{\nu+\mu+2j} | = | A^2\pi^2 + 2A\pi |. \tag{14.5}$$

The ordinal of the left hand side of equation (14.5) is odd and less than $2e$; that is, $| A^2\pi^2 + 2A\pi | > | \pi^{2e}$ and therefore $| A^2\pi^2 + 2A\pi | = | A^2\pi^2 |$. Hence the right hand side of equation (14.5) has an even ordinal. This contradiction establishes the contention.

Now we must deal with $\alpha\pi^{2e-\nu}$ and $\beta\pi^{2e-\nu}$. The α and β are integers; if $\alpha = \beta$, then $L \cong K$ and we are through. So assume that $\alpha \neq \beta$. Define an f such that $(\beta - \alpha)\pi^{-f}$ has ordinal either $-e$ or $-e-1$, the choice being made in such a way that $f + \nu$ is even. Clearly $f \geqq e > \nu$. Define a new

metric space $V^* = F \cdot \zeta \oplus V$ with $\zeta^2 = (\beta - \alpha)\pi^{-f}$ and put $L^* = \mathfrak{o}\zeta \oplus L$ and $K^* = \mathfrak{o}\zeta \oplus K$. According to Theorem 5. 1 it suffices to prove that $L^* \cong K^*$. Write $L^* = \mathfrak{o}\zeta + \mathfrak{o}\xi_1 + \mathfrak{o}\Xi_2$ with $\Xi_2 = \xi_2 + \pi^r\zeta$ and $r = \frac{1}{2}(2e + f - \nu)$. Then $r \geqq e + 1$. Also $(\mathfrak{o}\xi_1 + \mathfrak{o}\Xi_2) \cong (\mathfrak{o}\eta_1 + \mathfrak{o}\eta_2)$ by the contention proved above and by choice of ζ and r. If we apply Lemma 2. 2 we can write $L^* = \mathfrak{o}(\zeta + a\xi_1 + b\Xi_2) \oplus (\mathfrak{o}\xi_1 + \mathfrak{o}\Xi_2)$ since it can easily be checked that a and b are integers. A determinantal argument shows that $\zeta^2 \cong (\zeta + a\xi_1 + b\Xi_2)^2$. Hence $L^* \cong K^*$. Hence $L \cong K$. Q. E. D.

COROLLARY 14. 3. *If* $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ *with* $\xi_1^2 = a_1\pi^\nu$, $\xi_1 \cdot \xi_2 = 1$, $\xi_2^2 = \{\pi^\gamma\}$, γ *being* $\geqq e + 1$, *and if* $K = \mathfrak{o}\eta_1 + \mathfrak{o}\eta_2$ *with* $\eta_1^2 = a_1\pi^\nu + \{\pi^e\}$, $\eta_1 \cdot \eta_2 = 1$, $\eta_2^2 = \{\pi^\gamma\}$, *then* $L \cong K$ *provided that* $d(L) \cong d(K)$.

Proof. Since $\gamma \geqq e + 1$ there is an integer δ such that $(\eta_1 + \delta\eta_2)^2 = a_1\pi^\nu$. The result then follows from Theorem 14. 3.

LEMMA 14. 4. *If* $L \cong K \pmod{\pi^{2e-\nu+1}}$, *then* $L \cong K$. *This result also holds when* $\nu = e$.

Proof. Case 1. $\nu \neq e$: We can write $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ with $\xi_1^2 = \epsilon_1\pi^\nu$, $\xi_1 \cdot \xi_2 = 1$, $\xi_2^2 = \epsilon_2\pi^\nu$ where ϵ_1 and ϵ_2 are units. Since $K \cong L \pmod{\pi^{2e-\nu+1}}$, it is easy to see that K can be written as $\mathfrak{o}\eta_1 + \mathfrak{o}\eta_2$ with $\eta_1^2 = \epsilon_1\pi^\nu + \{\pi^{2e-\nu+1}\}$, $\eta_1 \cdot \eta_2 = 1$, $\eta_2^2 = \epsilon_2\pi^\nu + \{\pi^{2e-\nu+1}\}$. Successive application of Theorem 14. 3 and Hensel's lemma yields

$$K \cong \begin{pmatrix} \epsilon_1\pi^\nu + \{\pi^{2e-\nu+1}\} & 1 \\ 1 & \epsilon_2\pi^\nu + \{\pi^{2e-\nu+1}\} \end{pmatrix} \cong \begin{pmatrix} \epsilon_1\pi^\nu + \{\pi^{2e-\nu+1}\} & 1 \\ 1 & \epsilon_2\pi^\nu \end{pmatrix} \cong L.$$

Case 2. $\nu = e$: The same argument applies if $d(L) \not\cong -1$. If $d(L) \cong -1$, then $d(K) \cong -1$, and the result follows from the result on maximal lattices [11].

15. Congruence of lattices. Although we will not have occasion to refer to it in this paper (in view of the sharper results at our disposal for lattices of unit determinant) we mention here a useful application of Section 14 to lattices of arbitrary determinant. It follows from Lemma 14. 4 that if $L \cong K \pmod{\pi^{2e+1}}$, then $L \cong K$; this is also true for 1-dimensional lattices. Hence we obtain by induction the following result of Durfee [3, Theorem 2]:

THEOREM 15. 1. *If* L *and* K *are lattices in the same space and of least divisor* $|\pi^m|$, *then* $L \cong K$ *if* $L \cong K \pmod{\pi^{2e+m+1}}$.

16. Four-dimensional lattices. Having completed the two-dimensional case, we now concentrate on the four-dimensional improper case. We continue to use the same notation for ν. First some lemmas:

LEMMA 16. 1. *If X and Y are orthogonal vectors in the integral lattice L and if $X^2 = [\pi^p]$, $Y^2 = [\pi^q]$, $q + p$ being odd and $q < p$, then there is a unit α and a $\beta \,\varepsilon\, (\pi^{\frac{1}{2}(p-q+1)}) \cdot \mathfrak{o}$ such that $(\alpha X + \beta Y)^2 = \pi^p + \{\pi^{2e+q}\}$.*

Proof. By Lemma 4. 1 there is an α_0 such that $(\alpha_0 X)^2 = \pi^p + \{\pi^{p+1}\}$. Suppose that we have found α and β such that $(\alpha X + \beta Y)^2 = \pi^p + \epsilon\pi^r$ with the greatest possible r: to prove that $r \geqq 2e + q$. Let us assume that $r < 2e + q$; we will establish a contradiction by producing a new α and β with a bigger r. Case 1: $r + p$ is even: By Lemma 4. 1 there is a unit A such that $A^2\pi^{r-p}X^2 \equiv \epsilon\pi^r \pmod{\pi^{r+1}}$. Then $((\alpha + A\pi^{\frac{1}{2}(r-p)}) \cdot X + \beta Y)^2 = \pi^p + \{\pi^{r+1}\}$, by choice of A and since $| 2\alpha A \pi^{\frac{1}{2}(r-p)} \cdot X^2 | < | \pi^r |$, r being less than $p + 2e$. This denies the maximality of r. Case 2: $r + q$ is even. This follows in the same way as Case 1. Q. E. D.

LEMMA 16. 2. *Under the same assumptions as Lemma 16. 1, there exists a unit β and an integer α such that $(\alpha X + \beta Y)^2 = a_1\pi^q + \{\pi^{2e+q}\}$, provided that $Y^2 = a_1\pi^q + \{\pi^p\}$ where a_1 is a unit.*

Proof. Similar to proof of Lemma 16. 1.

A special change of basis. Let $L = (\mathfrak{o}X_1 + \mathfrak{o}X_2) \oplus (\mathfrak{o}X_3 + \mathfrak{o}X_4)$ be an improper totally integral lattice of unit determinant. Consider the following changes of basis in which $| \epsilon | = 1$ and $\alpha \,\varepsilon\, \mathfrak{o}$:

$$L = \mathfrak{o}X_1 + \mathfrak{o}X_2 + \mathfrak{o}(\epsilon X_3 + \alpha X_1) + \mathfrak{o}X_4 = (\mathfrak{o}Y_1 + \mathfrak{o}Y_2) \oplus (\mathfrak{o}Y_3 + \mathfrak{o}Y_4)$$

where $Y_1 = X_1 + AY_3 + BY_4$; $Y_2 = X_2 + A'Y_3 + B'Y_4$; $Y_3 = \epsilon X_3 + \alpha X_1$; $Y_4 = X_4$, the (integers) A, A', B, B', being determined by Lemma 2. 2. We denote this change of basis from (X_i) to (Y_i) by the symbol $\mathrm{op}(X_3 \to \epsilon X_3 + \alpha X_1)$ and write $Y_i = \mathrm{op}(X_i)$; this symbol is defined for any unit ϵ and for any integer α; in fact we can make preliminary estimates on the magnitudes of the A's and B's by solving the equations of Lemma 2. 2 to obtain

$$\begin{aligned} | A | &= | \alpha \cdot X_1^2 \cdot X_4^2 | \quad ; \quad | B | = | \alpha \cdot X_1^2 | \\ | A' | &= | \alpha \cdot X_4^2 \cdot | \quad ; \quad | B' | = | \alpha |. \end{aligned} \tag{16. 1}$$

Observe that $\mathrm{op}(X_1) \cdot \mathrm{op}(X_2)$ is a unit.

Definition 16. 1. A two-dimensional lattice is a null lattice if it has a basis $L = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ for which $\xi_1^2 = 0 = \xi_2^2$ and $\xi_1 \cdot \xi_2 = 1$.

Notation. If L is any totally integral lattice of unit determinant, $\dim L \geqq 3$, $N(L) = (\pi^\nu)\cdot\mathfrak{o}$, $0 \leqq \nu \leqq e$, we define $\mu = \min \operatorname{ord} X^2$, the minimum being over all X in L having the property $\operatorname{ord} X^2 + \nu$ is odd, provided that the μ obtained exists and is less than e; otherwise take $\mu = e$. When there is any risk of misunderstanding we will write $\mu(L)$ for μ. Note that if $\mu + \nu$ is even, then μ must be e.

LEMMA 16. 3. *There is a decomposition $L = L_0 \oplus L_1$ for L such that*

$$L_0 \cong \begin{pmatrix} [\pi^\nu] & 1 \\ 1 & \{\pi^\gamma\} \end{pmatrix} \text{ and } L_1 \cong \begin{pmatrix} \pi^\mu & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix} \tag{16.2}$$

in which (1) *L_1 is null and $\gamma \geqq e+1$ when $\mu+\nu$ is even;* (2) *$\gamma \geqq \mu$ when $\mu + \nu$ is odd.*

Proof. There is a basis $L = (\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2) \oplus (\mathfrak{o}\xi_3 + \mathfrak{o}\xi_4)$ in which (by Lemmas 4. 3, 2. 2)

$$\xi_1^2 = [\pi^\nu]\,;\ \xi_1\cdot\xi_2 = 1\,;\ \text{and}\ \xi_2^2\ \varepsilon\ \{\pi^\nu\}. \tag{16.3}$$

The second component can then be made to take the form $\xi_3^2 = [\pi^\lambda]$; $\xi_3\cdot\xi_4 = 1$; $\xi_4^2\ \varepsilon\ (\pi^\mu)\cdot\mathfrak{o}$ in virtue of Lemma 14. 1. Of all minimal bases (ξ) satisfying the equations (16. 3) and having $\xi_4^2\ \varepsilon\ (\pi^\mu)\cdot\mathfrak{o}$, choose one for which λ is greatest (possibly ∞). Then $\lambda \geqq \mu$. For if not, $\lambda + \nu$ would be even by definition of μ; then there would be an $\alpha_0\ \varepsilon\ \mathfrak{o}$ such that $(\xi_3 + \alpha_0\cdot\xi_1)^2\ \varepsilon\ (\pi^{\lambda+1})\cdot\mathfrak{o}$; apply $\operatorname{op}(X_3 \to X_3 + \alpha X_1)$ on this basis with $\alpha = \alpha_0$; then $(\operatorname{op}(X_1))^2 = [\pi^\nu]$ by equations (16. 1). This is a contradiction and so $\lambda \geqq \mu$.

Case 1. $\mu = e$ and $\nu + e$ is even: Then $\lambda > e$ and $(\mathfrak{o}\xi_3 + \mathfrak{o}\xi_4)$ is therefore null. Applying Lemma 14. 1 to $(\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2)$ completes the proof of this case.

Case 2. $\mu + \nu$ is odd: We first show how to achieve $\lambda = \mu$ by suitable changes of basis. If $(\mathfrak{o}\xi_3 + \mathfrak{o}\xi_4)$ represents $[\pi^\mu]$ (e. g. when $\mu = e$), we are through. If not, then $(\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2)$ must represent $[\pi^\mu]$ and we can therefore write $\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2 = \mathfrak{o}\eta_1 + \mathfrak{o}\eta_2$ with $\eta_1^2 = [\pi^\nu]$; $\eta_1\cdot\eta_2 = 1$; $\eta_2^2 = [\pi^\mu]$ in virtue of Lemma 14. 1. If we apply $\operatorname{op}(X_3 \to X_3 + X_2)$ to the basis $(\eta_1, \eta_2, \xi_3, \xi_4)$ we obtain

$$L \cong \begin{pmatrix} [\pi^\nu] & 1 \\ 1 & \{\pi^\nu\} \end{pmatrix} \oplus \begin{pmatrix} \delta\pi^\mu & 1 \\ 1 & [\pi^\beta] \end{pmatrix}, \qquad |\,\delta\,| = 1 \tag{16.4}$$

in the basis $(\zeta_1, \zeta_2, \zeta_3, \zeta_4)$. Of all minimal bases (ζ) having the form of (16. 4), choose one having a maximal β. Then $\beta \geqq 2e - \mu$, for if $\beta < 2e - \mu$ then

$\beta + \mu$ would be odd by Lemma 14. 1, and an application of $\mathrm{op}(X_4 \to X_4 + \alpha X_1)$ with a suitable α would lead to a contradiction.

To show that δ can be taken equal to 1: by Lemma 16. 1 we can find a unit ϵ and an integer α such that $(\epsilon\zeta_3 + \alpha\zeta_1)^2 = \pi^\mu + \{\pi^{2e+\nu}\}$. Apply $\mathrm{op}(X_3 \to \epsilon X_3 + \alpha X_1)$ and call the first component L_0, the second L_1. Then L_0 has the required form by Lemma 14. 1; and L_1 has the required form by Lemma 14. 4. Q. E. D.

LEMMA 16. 4. *If L and K are lattices in the same metric space and have the forms*

$$(16.5a)\qquad \begin{pmatrix} a_1\pi^\nu & 1 \\ 1 & \{\pi^\nu\} \end{pmatrix} \oplus \begin{pmatrix} [\pi^\mu] & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix}$$

$$(16.5b)\qquad \begin{pmatrix} a_1\pi^\nu & 1 \\ 1 & \{\pi^\nu\} \end{pmatrix} \oplus \begin{pmatrix} \pi^\mu & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix}$$

respectively, and if $\mu + \nu$ is odd, then $L \cong K$.

Proof. Let L have the form (16. 5a) when written in the basis $L = (\mathfrak{o}\xi_1 + \mathfrak{o}\xi_2) \oplus (\mathfrak{o}\xi_3 + \mathfrak{o}\xi_4)$. By Lemma 16. 1 there is a unit ϵ and an $\alpha \in (\pi^{\frac{1}{2}(\mu-\nu+1)}) \cdot \mathfrak{o}$ such that $(\alpha\xi_1 + \epsilon\xi_3)^2 = \pi^\mu + \{\pi^{2e+\nu}\}$; apply $\mathrm{op}(X_3 \to \epsilon X_3 + \alpha X_1)$ to this basis with these values of α and ϵ. Then $(\mathrm{op}(X_3))^2 = \pi^\mu + \{\pi^{2e+\nu}\}$ and $(\mathrm{op}(X_1))^2 = a_1\pi^\nu + \{\pi^{2e}\}$ by equations (16. 1). Then applying Lemma 14. 4 to both of these new components for L shows that L can be written in the form (16. 5b). Call this decomposition $L = L_0 \oplus L_1$. Let $K = K_0 \oplus K_1$ be a decomposition of K corresponding to the form (16. 5b). In virtue of Theorem 14. 3 it suffices to prove that $d(L_0) \cong d(K_0)$ and $d(L_1) \cong d(K_1)$ and this amounts to proving that $d(L_1) \cong d(K_1)$ since $d(L) \cong d \cong d(K)$.

To prove $d(L_1) \cong d(K_1)$ we take S-symbols. Direct calculation shows that $1 \sim S(L) \cdot S(K) \sim (d(L_1) \cdot d(K_1), -a_1 d\pi)$. Utilizing the remark of Section 8 we see that this can only occur if $d(L_1) \cong d(K_1)$ since $d(L_1) \cdot d(K_1) = 1 + \{4\}$. Q. E. D.

THEOREM 16. 5. *If L and K are improper 4-dimensional lattices in the 4-dimensional metric space V and have the properties*: (1) $N(L) = (\pi^\nu) \cdot \mathfrak{o} = N(K)$; (2) $\mu(L) = \mu = \mu(K)$; (3) *corresponding to each Y in K with $Y^2 = [\pi^\nu]$, there is an X in L such that $X^2 \equiv Y^2 \pmod{\pi^\mu}$. Then $L \cong K$.*

Proof. We can assume that $e > \nu$. If $\mu + \nu$ is even, then $\mu = e$ and the result follows from Lemma 16. 3 and Corollary 14. 3; we can therefore assume that $\mu + \nu$ is odd. By Lemma 16. 3 we can write $K = K_1 \oplus K_0$ with

$$(16.6)\qquad K_1 \cong \begin{pmatrix} \pi^\mu & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix} \text{ and } K_0 \cong \begin{pmatrix} a_1\pi^\nu & 1 \\ 1 & a_2\pi^\lambda \end{pmatrix}$$

where a_1 and a_2 are units and $\lambda \geqq \mu$. Now apply Lemma 16. 3 to L to obtain $L = L_1 \oplus L_0$. Then L_0 must represent $a_1\pi^\nu + \{\pi^\mu\}$ since L represents this quantity and since $N(L_1) = (\pi^\mu) \cdot \mathfrak{o}$. Hence we can find bases $L_1 = \mathfrak{o}\xi_1 + \mathfrak{o}\xi_2$ and $L_0 = \mathfrak{o}\xi_3 + \mathfrak{o}\xi_4$ in which L has the form

$$(16.\,7) \qquad L \cong \begin{pmatrix} [\pi^\mu] & 1 \\ 1 & \{\pi^\nu\} \end{pmatrix} \oplus \begin{pmatrix} a_1\pi^\nu + \delta\pi^\mu & 1 \\ 1 & a_2\pi^\lambda + [\pi^\Gamma] \end{pmatrix}, \ \delta \,\varepsilon\, \mathfrak{o}$$

where $\mu \leqq \Gamma \leqq \infty$. By Lemma 16. 2 there is a unit ϵ and an integer α such that $(\epsilon\xi_3 + \alpha\xi_1)^2 = a_1\pi^\nu + \{\pi^{2e+\nu}\}$. Apply $\mathrm{op}(X_3 \to \epsilon X_3 + \alpha X_1)$ to the basis (ξ): then $(\mathrm{op}(X_1))^2 = [\pi^\mu]$ and $(\mathrm{op}(X_3))^2 = a_1\pi^\nu + \{\pi^{2e+\nu}\}$ by the equations (16. 1). Now apply Lemma 14. 4 to the resulting second component after the application of the above operation and we see that L has a basis (ζ) in which L has the form of equation (16. 7) with $\delta = 0$. Of all bases (ζ) having this form, choose one in which Γ is maximal. Then Γ must be $\geqq 2e - \nu$: for if $\Gamma < 2e - \nu$, then $\Gamma + \nu$ must be odd, using the argument of equation (14. 3); in that event, $\Gamma + \mu$ would be even and an application of $\mathrm{op}(X_4 \to \epsilon X_4 + \alpha X_1)$ would lead to a contradiction. Hence $\Gamma \geqq 2e - \nu$.

Hence we have $L = L_1^* \oplus L_0^*$ with $d(L_0^*) \cong d(K_0) \pmod 4$ and hence $d(L_1^*) \cong d(K_1) \pmod 4$ and hence $d(L_1^*) \cong -1 \pmod 4$. Now L_1^* represents $[\pi^\mu]$ and a determinantal consideration (compare Remark 14. 1) then shows that $L_1^* \cong \begin{pmatrix} [\pi^\mu] & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix}$. The proof of the theorem follows by applying Lemma 16. 4 to $L_0^* \oplus L_1^*$ and $K_0 \oplus K_1$.

17. The general improper case. We now consider general improper lattices L of unit determinant. Most of the labour has already been done and we need only show that the general case reduces to the case of dimension 4. By Theorem 2. 4 we can write $L = \sum L_\lambda$ where the L_λ are improper and of dimension 2. Then it is possible to write $L = L_1 \oplus L_2 \oplus \sum N_\lambda$ where L_1 and L_2 are of dimension 2 and the N_λ are null lattices: this can be achieved by successively applying $\mathrm{op}(X_i \to \epsilon X_i + \alpha X_j)$ but we have manipulated with this operation often enough to be able to omit the details of the proof.

Now let L and K be lattices of arbitrary dimension but otherwise satisfying the conditions of Theorem 16. 5. Reduce L and K to the forms $L_1 \oplus L_2 \oplus \sum N_\lambda$ and $K_1 \oplus K_2 \oplus \sum N_\lambda$. Then $L_1 \oplus L_2$ and $K_1 \oplus K_2$ are in isometric spaces [20] and also satisfy the remaining conditions of Theorem 16. 5. Hence they are isometric. *Hence Theorem* 16. 5 *holds for lattices of arbitrary dimension.*

18. The proper case. We carry over the notation for μ and ν: in this case ν will always be zero and μ can be even only when $\mu = e$. The proper case will be made to depend on the improper case. We state without proof the fact that a proper lattice $L = \mathfrak{o}\xi_1 \oplus \cdots \oplus \mathfrak{o}\xi_n$ with $|\xi_i^2| = 1$ can be written

$$L = L_1 \oplus L_2 \oplus \sum N_\lambda \tag{18.1}$$

where L_1 is proper and of dimension $\leqq 2$, the N_λ are all null and L_2 is of the form $\begin{pmatrix} \pi^\mu & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix}$ when μ is odd, and is the null lattice when μ is even: the proof is similar to the argument of Lemma 16.3.

LEMMA 18.1. *If L and K are proper lattices of unit determinant and of odd dimension in the same metric space V and if $\mu(L) = \mu(K)$, then $L \cong K$.*

Proof. If μ is even the proof is immediate from equation (18.1). So assume that μ is odd. Again referring to equation (18.1), we can write $L = \mathfrak{o}\xi_1 \oplus (\mathfrak{o}\xi_2 + \mathfrak{o}\xi_3) \oplus \sum N_\lambda$ and $K = \mathfrak{o}\eta_1 \oplus (\mathfrak{o}\eta_2 + \mathfrak{o}\eta_3) + \sum N_\lambda$. In fact we will prove that $\mathfrak{o}\xi_1 \oplus (\mathfrak{o}\xi_2 + \mathfrak{o}\xi_3)$ and $\mathfrak{o}\eta_1 \oplus (\mathfrak{o}\eta_2 + \mathfrak{o}\eta_3)$ are isometric, so let us denote these by L and K and assume that $\dim V = 3$.

Define an integer f equal to e or $e+1$, the choice being such that f is odd. Construct the new metric space $V^* = F\cdot\zeta \oplus V$ with $\zeta^2 = \pi^{-f}$ and put $L^* = \mathfrak{o}\zeta \oplus L$ and $K^* = \mathfrak{o}\zeta \oplus K$. By Theorem 5.1 it suffices to prove $L^* \cong K^*$.

By Lemma 4.1 there is an integer α such that $(\xi_3 + \alpha\pi^r\zeta)^2 \varepsilon (\pi^{2e-\mu+1})\cdot\mathfrak{o}$ where $2r = 2e - \mu + f$. Write $L^* = \mathfrak{o}\xi_1 \oplus (\mathfrak{o}\zeta + \mathfrak{o}\xi_2 + \mathfrak{o}\Xi_3)$ where $\Xi_3 = \xi_3 + \alpha\pi^r\zeta$. Then the equations of Lemma 2.2 have integral solutions when applied to $\mathfrak{o}\xi_3 + \mathfrak{o}\Xi_3$ and we can write $L^* = \mathfrak{o}\xi_1 \oplus \mathfrak{o}Z \oplus (\mathfrak{o}\xi_2 + \mathfrak{o}\Xi_3)$ where $d(\mathfrak{o}\xi_2 + \mathfrak{o}\Xi_3) \cong -1$. Similarly $K^* = \mathfrak{o}\eta_1 \oplus \mathfrak{o}Y \oplus (\mathfrak{o}\eta_2 + \mathfrak{o}H_3)$. Then $\mathfrak{o}\xi_2 + \mathfrak{o}\Xi_3 \cong \mathfrak{o}\eta_2 + \mathfrak{o}H_3$ by Theorem 14.3. Let $Z^2 = \epsilon_1\pi^{-f}$ and $\xi_1^2 = \epsilon_2$; then a determinantal consideration shows that $Y^2 = \epsilon_1\delta\pi^{-f}$ and $\eta_1^2 = \epsilon_2\delta$ where $\delta = 1 + \{4\}$. Now the S-symbols of $\mathfrak{o}\xi_1 \oplus \mathfrak{o}Z$ and $\mathfrak{o}\eta_1 \oplus \mathfrak{o}Y$ must be equal and direct computation yields $1 \sim (\delta, \pi)$ and δ must therefore be a square by Section 8. Q. E. D.

LEMMA 18.2. *If L and K are of even dimension, then $L \cong K$ provided that (1) $\mu(L) = \mu(K)$; (2) L and K represent the same units.*

Proof. Since L and K are in the same metric space, there is nothing to prove when $n = 2$. So assume that $n \geqq 4$. By a slight modification to

equation (18. 1) we can write L in the form of equation (18. 1) with L_2 of the form $\begin{pmatrix} \pi^\gamma & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix}$ where $\gamma = \mu$ when μ is odd and $\gamma = e + 1$ (and is therefore odd) when μ is even. Then

$$(18.2) \qquad L \cong (a) \oplus (b) \oplus \begin{pmatrix} \pi^\gamma & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix} \oplus \Sigma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

in the basis (ξ). Then of all bases (η) for K having the form of equation (18. 3), choose one in which Δ is maximal:

$$(18.3) \qquad K \cong (a + [\pi^\Delta]) \oplus (c) \oplus \begin{pmatrix} \pi^\gamma & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix} \oplus \Sigma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Contention: $\Delta = \infty$. For Δ must be $\geqq \mu$ since $\mathfrak{o}\eta_1 + \mathfrak{o}\eta_2$ represent $a \pmod{\pi^\mu}$; and Δ cannot be even, for we could then write $\mathfrak{o}\eta_1 \oplus \mathfrak{o}\eta_2 = \mathfrak{o}(\eta_1 + \alpha\eta_2) \oplus \mathfrak{o}H_2$ with α so chosen (by Lemma 4. 1) that $(\eta_1 + \alpha\eta_2)^2 \equiv a \pmod{\pi^{\Delta+1}}$; it remains to consider Δ odd and $\geqq \gamma$; we could then write $\mathfrak{o}\eta_1 \oplus (\mathfrak{o}\eta_3 + \mathfrak{o}\eta_4) = \mathfrak{o}(\eta_1 + \alpha\eta_3) \oplus K_1{}^*$ so that $(\eta_1 + \alpha\eta_3)^2 \equiv a \pmod{\pi^{\Delta+1}}$ by Lemmas 4. 1 and 2. 1 and it is easy to verify that $\mu(\mathfrak{o}\eta_3 + \mathfrak{o}\eta_4) = \mu(K_1{}^*)$ and hence (equation 18. 1) that $\mathfrak{o}\eta_2 \oplus K_1{}^*$ could be written in a basis having the form $[1] \oplus \begin{pmatrix} \pi^\gamma & 1 \\ 1 & \{\pi^{2e-\mu}\} \end{pmatrix}$. Hence Δ must be ∞ in the basis (η). Then we can apply Lemma 18. 1 to $\mathfrak{o}\xi_2 + \cdots + \mathfrak{o}\xi_n$ and $\mathfrak{o}\eta_2 + \cdots + \mathfrak{o}\eta_n$. Hence $L \cong K$.
Q. E. D.

19. Piecing together Section 17, Lemma 18. 1 and Lemma 18. 2 proves

THEOREM 19. 1. *If L and K are totally integral lattices of unit determinant in the same metric space V, then L is isometric to K provided that L and K represent the same numbers.*

20. Appendix. We have constantly used the invariants of [20, Satz 17]; these were shown by Witt to hold over any field in which every form of five or more variables is a zero form; e. g. over a local field with finite residue class field; compare also the result of Kaplansky. We now prove that the latter property is also true for a local field having a perfect residue class field of characteristic 2.

Proof. Let $l = \sum_1^5 a_i x_i^2$ be given in diagonal form. By considering $\pi \cdot l$ if necessary, we can assume that at least three of the a_i are units and

that the remaining two (a_4 and a_5 say) are either units or primes. Construct a metric space V and a lattice L in V corresponding to l: $L = \mathfrak{o}\xi_1 \oplus \cdots \oplus \mathfrak{o}\xi_5$. If $|a_i| = 1$ all i, the result follows from equation (18.1). If $|a_4| = |\pi|$, by applying equation (18.1) to $\mathfrak{o}\xi_1 \oplus \mathfrak{o}\xi_2 \oplus \mathfrak{o}\xi_3$, we can write

$$L = \mathfrak{o}\eta_1 \oplus (\mathfrak{o}\eta_2 + \mathfrak{o}\eta_3) \oplus \mathfrak{o}\eta_4 \oplus \mathfrak{o}\eta_5 \tag{20.1}$$

with $|\eta_1^2| = 1$; $\eta_2 \cdot \eta_3 = 1$; $\eta_2^2, \eta_3^2 \in (\pi) \cdot \mathfrak{o}$; and $|\eta_4^2| = |\pi|$. Of all bases (η) having the form of equation (20.1), choose one in which $|\eta_2^2|$ is minimal. Then it follows from the fact that $\operatorname{ord} \eta_1^2 = 0$ and $\operatorname{ord} \eta_4^2 = 1$ and from Lemma 2.2, that $\eta_2^2 = 0$. Q. E. D.

Note that the proof just given (which rests on equation 18.1) depends solely on the operation $\operatorname{op}(X_i \to \epsilon X_i + \alpha X_j)$ and the fact that the residue class field is perfect and of characteristic 2.

PRINCETON UNIVERSITY, NEW JERSEY AND
OTAGO UNIVERSITY, NEW ZEALAND.

REFERENCES.

[1] E. Artin, "Algebraic numbers and algebraic functions I," *Princeton University, New York University*, 1950-1951.

[2] C. Chevalley, "L'Arithmétique dans les algèbres de matrices," *Actualités Scientifiques et Industrielles*, 323 (1936).

[3] W. H. Durfee, "Congruence of quadratic forms over valuation rings," *Duke Mathematical Journal*, vol. 11 (1944), pp. 687-697.

[4] ———, "Quadratic forms over fields with a valuation," *Bulletin of the American Mathematical Society*, vol. 54 (1948), pp. 338-351.

[5] H. Hasse, "Über die Äquivalenz quadratischer Formen im Körper der rationalen Zahlen," *Journal für die reine und angewandte Mathematik*, vol. 152 (1923), pp. 205-224.

[6] ———, "Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper," *Journal für die reine und angewandte Mathematik*, vol. 153 (1924), pp. 158-162.

[7] B. W. Jones, "An extension of a theorem of Witt," *Bulletin of the American Mathematical Society*, vol. 48 (1942), pp. 133-142.

[8] ———, "A canonical quadratic form for the ring of 2-adic integers," *Duke Mathematical Journal*, vol. 11 (1944), pp. 715-727.

[9] ———, "The Arithmetic Theory of Quadratic Forms," *Carus Monographs*, No. 10, Mathematical Association of America, 1950.

[10] ——— and W. H. Durfee, "A theorem on quadratic forms over the ring of 2-adic integers," *Bulletin of the American Mathematical Society*, vol. 55 (1949), pp. 758-762.

[11] M. Eichler, "Quadratische Formen und orthogonale Gruppen," Berlin (1952).

[12] ———, "Note zur Theorie der Kristallgitter," *Mathematische Annalen*, vol. 125 (1952), pp. 51-55.

[13] I. Kaplansky, "Quadratic Forms," *Journal of the Mathematical Society of Japan*, vol. 5 (1953), pp. 200-207.

[14] M. Kneser, "Zur Theorie der Kristallgitter," *Mathematische Annalen*, vol. 127 (1954), pp. 105-106.

[15] G. Pall, "The arithmetical invariants of quadratic forms," *Bulletin of the American Mathematical Society*, vol. 51 (1945), pp. 185-197.

[16] ———, "On the order invariants of integral quadratic forms," *Quarterly Journal of Mathematics*, vol. 6 (1935), pp. 30-51.

[17] H. Minkowski, *Gesammelte Abhandlungen* I (1911).

[18] C. Siegel, "Equivalence of quadratic forms," *American Journal of Mathematics*, vol. 63 (1941), pp. 658-680.

[19] B. L. van der Waerden, "Modern Algebra," New York (1949).

[20] E. Witt, "Theorie der quadratischen Formen in beliebigen Körpern," *Journal für die reine und angewandte Mathematik*, vol. 176 (1937), pp. 31-44.

AUTOMORPHISMS OF FINITE FACTORS.*

By I. M. Singer.

1. Introduction and notation. Let $\mathfrak{G}$ be a countable group of point measure preserving transformations on a non-atomic separable measure space $(X, \boldsymbol{F}, \mu)$, where X is the underlying space, $\boldsymbol{F}$ the σ-Boolean algebra of measurable sets and μ the measure. If $x \,\varepsilon\, X$ and $g \,\varepsilon\, \mathfrak{G}$, xg will denote the action of $\mathfrak{G}$ on X; and if E is any subset of X, $Eg = [xg; x \,\varepsilon\, E]$. Assume that (1.1) $\mu(X) = 1$. (1.2) if $E \,\varepsilon\, \boldsymbol{F}$, $\mu(E) \neq 0$, and g is not the identity of $\mathfrak{G}$, then there exists a subset $F \,\varepsilon\, \boldsymbol{F} \ni F \subset E$, $\mu(F) \neq 0$, and $\mu(F \,\Delta\, Fg) \neq 0$. (1.3) $\mathfrak{G}$ acts ergodically on $(X, \boldsymbol{F}, \mu)$; i.e., if $E \,\varepsilon\, \boldsymbol{F}$ and $\mu(E \,\Delta\, Eg) = 0$ for all $g \,\varepsilon\, \mathfrak{G}$, then $\mu(E) = 0$ or $\mu(E) = 1$. (Δ denotes the symmeric difference; this second condition means that an element of $\mathfrak{G}$, not the identity, is not the identity on any piece of X of positive measure.)

Associated with this action of $\mathfrak{G}$ on $(X, \boldsymbol{F}, \mu)$, F. J. Murray and J. von Neumann ([7] pp. 192-209) constructed a finite factor as follows: Let $\mathfrak{H} =$ [set of all complex valued functions ξ on $\mathfrak{G} \times X \ni$ for each $g \,\varepsilon\, \mathfrak{G}$, $\xi_g(x) = \xi(g, x) \,\varepsilon\, L_2(X, \boldsymbol{F}, \mu)$ and $\sum_{g \,\varepsilon\, \mathfrak{G}} \| \xi_g(x) \|_2^2 < \infty$, where $\| \cdot \|_2$ is the L_2 norm on $(X, \boldsymbol{F}, \mu)$.] It is not hard to see that $\mathfrak{H}$ is a separable Hilbert space, the inner product (ξ, η) of two functions ξ and η being $\sum_{g \,\varepsilon\, \mathfrak{G}} \int_X \xi(g, x) \bar{\eta}(g, x) d\mu$. In fact, $\mathfrak{H} = L_2(X \times \mathfrak{G})$ where the measure on $X \times G$ is the product of μ and Haar measure on $\mathfrak{G}$. Let $\mathfrak{B} = [\xi \,\varepsilon\, \mathfrak{H}; \xi(g, x) = 0$ except for a finite number of $g \,\varepsilon\, \mathfrak{G}$, and for each g, $\xi(g, x)$ is a bounded measurable function on $X]$. The following convolution-like product can be defined for $\eta \,\varepsilon\, \mathfrak{H}$ and $\xi \,\varepsilon\, B$: $\eta\xi(g, x) = \sum_{h \,\varepsilon\, \mathfrak{G}} \eta(h, x) \xi(gh^{-1}, xh^{-1})$, and $\eta\xi \,\varepsilon\, \mathfrak{H}$. If η has the property that $\| \eta\xi \| \leqq K \| \xi \|$ for all $\xi \,\varepsilon\, B$, then η can be extended to be a bounded operator L_η on $\mathfrak{H}$. The set $\mathfrak{L}$ of such L_η is a finite factor; moreover, $L_{\alpha_1\eta_1 + \alpha_2\eta_2} = \alpha_1 L_{\eta_1} + \alpha_2 L_{\eta_2}$; $L_{\eta_1\eta_2} = L_{\eta_1} L_{\eta_2}$ and $(L_\eta)^* = L_{\eta^*}$ where $\eta^*(g, x) = \bar{\eta}(g^{-1}, xg^{-1})$. Similarly, one can define the algebra of bounded right multiplications $\mathfrak{R}$ where $R_\eta \,\varepsilon\, \mathfrak{R}$ if $\| R_\eta \xi \| = \| \xi\eta \| \leqq K \| \xi \|$, $\xi \,\varepsilon\, \mathfrak{B}$. $\mathfrak{R}$ and $\mathfrak{L}$ are the commutants of one another; also the set $\mathfrak{B}_1$ of all bounded elements on the left equals the set of all bounded elements on the right, and the map

* Received March 9, 1954.

$L_\xi \rightarrow R_\xi$ of $\mathcal{L}$ into $\mathcal{R}$ is an anti-isomorphism of these two $*$-algebras. All these facts are proved in ([1] pp. 192-209).

From a different point of view [1], the algebraic system consisting of $\mathfrak{H}$ together with multiplication of its elements (wherever the product makes sense and lies in $\mathfrak{H}$) forms a simple H-system with identity. For the connections between these two viewpoints and other descriptions of this algebra see [2], [3], and [10]. Since both points of view have advantages, we will pass from one to the other freely. For us, then, $\mathfrak{H}$ will denote the Hilbert space together with the above defined multiplication and adjoint.

Let $\mathcal{A} = [\xi \,\varepsilon\, \mathfrak{H}; \xi(g,x) = 0, g \neq e]$. $\mathcal{A}$ is a maximal abelian subalgebra of the H-system $\mathfrak{H}$ identifiable with the H-system $L_2(X, \boldsymbol{F}, \mu)$ under pointwise multiplication; $\mathcal{A} \cap \mathcal{B}_1$ can be identified with the set of essentially bounded measurable functions on $(X, \boldsymbol{F}, \mu)$. These identifications are made via the mapping: $\xi \rightarrow \xi(e,x)$. Conversely, if $a(x)$ is a bounded measurable function, let ξ^a be that element of $\mathcal{A} \ni \xi^a(e,x) = a(x)$; let $\mathcal{L}_{\mathcal{A}} = \{L_{\xi^a}\}$ and let $\mathcal{R}_{\mathcal{A}} = \{R_{\xi^a}\}$. To make the notation less cumbersome when there is little chance for confusion, we will identify ξ^a and the function $a(x)$. The restriction of the anti-isomorphism of $\mathcal{L}$ onto $\mathcal{R}$ is an isomorphism of $\mathcal{L}_{\mathcal{A}}$ onto $\mathcal{R}_{\mathcal{A}}$ since they are abelian.

In this paper, we analyze the group $\mathfrak{S}$ of those automorphisms of the H-system $\mathfrak{H}$ sending $\mathcal{A}$ into $\mathcal{A}$. Since the entire H-system $\mathfrak{H}$ was constructed out of the action of $\mathfrak{G}$ on X, i. e., $\mathfrak{G}$ on $\mathcal{A}$ $(\cong L_2(X))$, one would expect that a description of $\mathfrak{S}$ can be given entirely in terms of this action; in fact, we do succeed in describing $\mathfrak{S}$ in terms of the subgroup $\mathfrak{G}$ of the entire group of measure preserving transformations of $(X, \boldsymbol{F}, \mu)$. Questions about $\mathfrak{S}$ can be reduced to questions directly concerned with measure preserving transformations. We can answer some of these questions, but not others.

2. Preliminary lemmas. We devote this section to a series of computational lemmas showing what various operators on $\mathfrak{H}$ look like.

Since $\mathfrak{H}$ is, as a Hilbert space, isomorphic to a countable direct sum (indexed by elements of $\mathfrak{G}$) of $L_2(X, \boldsymbol{F}, \mu)$, any bounded operator T on $\mathfrak{H}$ can be decomposed into an infinite matrix $\{T_{g,h}\}$, $g, h \,\varepsilon\, \mathfrak{G}$, where $T_{g,h}$ is a bounded operator on $L_2(X, \boldsymbol{F}, \mu)$, and $(T\xi)(g,x) = \sum_{h \varepsilon \mathfrak{G}} (T_{g,h}\xi_h)(x)$. (Remember that ξ_h is that element of $L_2(X, \boldsymbol{F}, \mu) \ni \xi_h(x) = \xi(h,x)$.) One can easily check that if $S \sim \{S_{g,h}\}$ and $T \sim \{T_{g,h}\}$ then

$$\alpha S + \beta T \sim \{\alpha S_{g,h} + \beta T_{g,h}\} \quad \text{and} \quad ST \sim \{\sum_{k \varepsilon \mathfrak{G}} S_{g,k} T_{k,h}\},$$

this last sum converging in the strong operator topology. We now compute the matrices corresponding to several bounded operators.

2.1 LEMMA. *If* $\xi^a \varepsilon \mathcal{A} \cap \mathcal{B}_1$, *then* $\xi^a\eta(g,x) = L_{\xi^a}(\eta)(g,x) = a(x)\eta(g,x)$ *and* $L_{\xi^a} \sim \{T_{g,h}\}$ *where* $T_{g,h} = 0$ *if* $g \neq h$ *and* $T_{g,g}$ *for any* $g \varepsilon \mathfrak{G}$ *is multiplication by the function* $a(x)$ *on* $L_2(X, \mathbf{F}, \mu)$. *Also* $\eta\xi^a(g,x) = R_{\xi^a}(\eta)(g,x) = a(xg^{-1})\eta(g,x)$ *and* $R_{\xi^a} \sim \{T_{g,h}\}$ *where* $T_{g,h} = 0$ *if* $g \neq h$ *and* $T_{g,g}$ *is multiplication by the function* $a(xg^{-1})$ *on* $L_2(X, \mathbf{F}, \mu)$.

Proof. The lemma follows directly from the definition of multiplication and the definition of ξ^a.

If $\tau \varepsilon \mathfrak{A}$ is a unitary element ($\tau^*\tau = \tau\tau^* = I$), then it leads to the inner automorphism J_τ where $J_\tau(\eta) = \tau\eta\tau^*$. We are interested in those J_τ leaving $\mathcal{A}$ invariant.

2.2 LEMMA. *Let* $E_g^\tau = [x \varepsilon X; \tau(g,x) \neq 0]$. *A necessary and sufficient condition that* τ *be a unitary element* $\ni \tau\mathcal{A}\tau^* = \mathcal{A}$ *is that the* E_g^τ *satisfy the following conditions*:

(i) $\mu(\bigcup_{g \varepsilon \mathfrak{G}} E_g^\tau) = 1$

(ii) if $g \neq h$, $\mu(E_g^\tau \cap E_h^\tau) = 0$

(iii) if $g \neq h$, $\mu(E_g^\tau g^{-1} \cap E_h^\tau h^{-1}) = 0$

(iv) $\sum_{h \varepsilon \mathfrak{G}} |\tau(h,x)|^2 = 1$ a. e. on X; and $|\tau(g,x)| = 1$, $x \varepsilon E_g^\tau$.

Proof. Suppose τ is unitary. Then $\tau\tau^* = I$ so that

$$\sum_{h \varepsilon \mathfrak{G}} \tau(h,x)\tau^*(gh^{-1}, xh^{-1}) = \sum_{h \varepsilon \mathfrak{G}} \tau(h,x)\tau(hg^{-1}, xg^{-1}) = 0$$

a. e. if $g \neq e$ and $\sum_{h \varepsilon \mathfrak{G}} |\tau(h,x)|^2 = 1$ a. e., proving the first part of (iv).

Since $\tau\mathcal{A} = \mathcal{A}\tau$, no matter what bounded measurable function $a(x)$ we choose, there exists a similar function $b(x) \ni \tau\xi^a = \xi^b\tau$. This means

$$\tau\xi^a(g,x) = a(xg^{-1})\tau(g,x) = b(x)\tau(g,x) = \xi^b\tau$$

(from 2.1); that is $a(xg^{-1}) = b(x)$ a. e. for $x \varepsilon E_g^\tau$. Hence $a(xg^{-1}) = a(xh^{-1})$ for almost all $x \varepsilon E_g^\tau \cap E_h^\tau$, and all bounded measurable functions $a(x)$. We now show that $\mu(E_g^\tau \cap E_h^\tau) = 0$ if $g \neq h$. For otherwise, by (1.2), there exists a set $F \subset E_g^\tau \cap E_h^\tau \ni \mu(F \Delta Fgh^{-1}) \neq 0$, so that $\mu(F \cap (Fg^{-1}h)') \neq 0$. Let $a(x)$ be the characteristic function of the set Fg^{-1}. $x \varepsilon F$ if and only if $xg^{-1} \varepsilon Fg^{-1}$ if and only if $a(xg^{-1}) \neq 0$. On the other hand $a(xh^{-1}) = 1$ if and only if $x \varepsilon Fg^{-1}h$; this means $a(xg^{-1}) = 1 \neq a(xh^{-1})$ if $x \varepsilon F \cap (Fg^{-1}h)'$. But $F \cap (Fg^{-1}h)' \subset F \subset E_g^\tau \cap E_h^\tau$, a contradiction.

Since $\sum_{h \varepsilon \mathfrak{G}} |\tau(h,x)|^2 = 1$ a. e. and (ii) holds, (i) and the second part of (iv) follow immediately.

For almost all $x \varepsilon X$, (i) and (ii) imply x lies in exactly one $E_g{}^\tau$. Then, if $g \neq e$, the first equation in this proof says $0 = \sum_h \tau(h, x)\bar{\tau}(hg^{-1}, xg^{-1})$ a. e. Thus for almost all $x \varepsilon E_k{}^\tau$, $0 = \tau(k, x)\bar{\tau}(kg^{-1}, xg^{-1})$ a. e., i. e., $\mu(E_k{}^\tau \cap E_{kg^{-1}}{}^\tau g) = 0$ if $g \neq e$. Let $h = kg^{-1}$ and let $\mu(E_k{}^\tau \cap E_h{}^\tau h^{-1}k) = 0$. Since k is measure preserving, $\mu(E_k{}^\tau k^{-1} \cap E_h{}^\tau h^{-1}) = 0$ $k \neq h$.

Suppose now that τ satisfies the conditions (i)-(iv). Condition (iv) says essentially that $\sum_{h \varepsilon \mathfrak{G}} \tau_h(x)$ defines a bounded measurable function $a(x)$ of absolute value 1 a. e. We can write $\tau = \xi^a \tau_1$, where $\tau_1(g, x) = e_g(x)$ and e_g is the characteristic function of the set $E_g{}^\tau$.

Since a is of absolute value 1, ξ^a is unitary. ξ^a leaves $\mathcal{A}$ invariant, so we need deal only with τ_1. It is not hard to show that τ_1 is unitary. We show that if $b(x)$ is bounded measurable, $\tau_1 \xi^b \tau_1{}^* \varepsilon \mathcal{A}$.

$$(\tau_1\xi^b)\tau_1{}^*(g, x) = \sum_{h \varepsilon \mathfrak{G}} \tau_1{}^*\xi^b(h, x)\bar{\tau}_1(hg^{-1}, xg^{-1})$$
$$= \sum_{h \varepsilon \mathfrak{G}} b(xh^{-1})\tau_1(hx)\bar{\tau}(hg^{-1}, xg^{-1}) = \sum_{h \varepsilon \mathfrak{G}} b(xh^{-1})e_h(x)e_{hg^{-1}}(xg^{-1}).$$

But if $g \neq e$, $E_h{}^\tau \cap E_{hg^{-1}}{}^\tau g$ is empty from (iii). Since $e_h(x)e_{hg^{-1}}(xg^{-1})$ is just the characteristic function of the set $E_h{}^\tau \cap E_{hg^{-1}}{}^\tau g$, we obtain $\tau\xi^b\tau^*(g, h) = 0$ a. e. if $g \neq e$ and $\tau\xi^b\tau^*(e, x) = \sum_h b(xh^{-1})e_h(x)$.

2. 3 Corollary. *If τ is a unitary element of $\mathfrak{H} \ni \tau\mathcal{A}\tau^* = \mathcal{A}$ then $\tau = \xi^a\tau_1$ where $a(x)$ is a measurable function of absolute value 1 on X, and where $\tau_1(g, x) = e_g(x)$ the characteristic functions of sets $E_g{}^\tau$ satisfying (i)-(iii) above. This decomposition is unique. Moreover, the automorphism J_τ on the H-system $\mathcal{A}$ is the same as that induced by the following point measure preserving transformation J_τ' defined a. e. If $x \varepsilon E_g{}^\tau g^{-1}$, then $xJ_\tau' = xg$.*

Proof. All but the last statement follows from the previous proof. Suppose now $b(x)$ is the characteristic function of a set F. Then by a previous formula, $\tau\xi^b\tau^* = \xi^d$ where $d(x) = \sum_h b(xh^{-1})e_h(x)$, i. e., $d(x)$ is the characteristic function of the set $\bigcup_h Fh \cap E_h{}^\tau$. This is exactly what J_τ' does to F, i. e., decomposes F into $\bigcup_h F \cap E_h{}^\tau h^{-1}$ and sends each $F \cap E_h{}^\tau h^{-1}$ into $(F \cap E_h{}^\tau h^{-1})h = Fh \cap E_h{}^\tau$.

The next lemma and corollary are contained in Lemma 2, p. 315 of Dixmier's paper [2]. We include the proofs for the sake of completeness.

2. 4 Lemma. *Let T be an operator on the Hilbert space $\mathfrak{H}$ which commutes with both $\mathcal{L}_\mathcal{A}$ and $\mathcal{R}_\mathcal{A}$. Then $T \sim \{T_{g,h}\}$ where $T_{g,h} = 0$ if $g \neq h$ and each $T_{g,g}$ is multiplication by a bounded measurable function $t_g(x)$.*

Proof. If $a(x)$ is bounded measurable, $T(\xi^a\eta)(g,x)=\xi^aT(\eta)(g,x)$; $\sum_h T_{g,h}(a(x)\cdot\eta(h,x))=a(x)\sum_h T_{g,h}\eta(h,x)$. If we choose η so that $\eta(h,x)=0$ except when $h=h'$, and $\eta(h',x)=b(x)$, we have $T_{g,h'}(a(x)b(x))=a(x)T_{g,h'}(b(x))$, i.e., $T_{g,h'}$ commutes with all multiplications by bounded measurable functions and hence is multiplication by one, $t_{g,h'}(x)$, itself.

Also $T(\eta\xi^a)(g,x)=T(\eta)\cdot\xi^a(g,x)$;

$$\sum_h t_{g,h}(x)a(xh^{-1})\eta(h,x)=a(xg^{-1})\sum_h t_{g,h}(x)\eta(h,x).$$

If we chose η as above,

$$t_{g,h'}(x)a(xh'^{-1})b(x)=a(xg^{-1})t_{g,h'}(x)b(x),$$

for all $a(x), b(x)$; $g, h'\in\mathfrak{G}$. Hence $t_{g,h}(x)(a(xh^{-1})-a(xg^{-1}))=0$. If $h\neq g$, and $F=[x;t_{g,h}(x)\neq 0]$ then for all functions $a(x)$, $a(xh^{-1})=a(xg^{-1})$, $x\in F$. As before (in the proof of (2.1)), condition (1.2) implies $\mu(F)=0$.

2.5 Corollary. $\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}}$, *the weakly closed algebra generated by* $\mathcal{L}_{\mathcal{A}}$ *and* $\mathcal{R}_{\mathcal{A}}$ *is a maximal abelian sub-algebra of all bounded operators.*[1]

Proof. Lemma 2.4 shows that the commutant $(\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}})'$ is abelian and hence $(\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}})'\subseteqq(\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}})''=\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}}$. On the other hand $\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}}$ is abelian, so $\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}}\subseteqq(\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}})'$.

2.6 Lemma. *Let* u_g, $g\in\mathfrak{G}$ *be the element* $\ni u_g(h,x)=0$ *if* $h\neq g$, $u_g(g,x)=1$, $x\in X$. *Then* $u_gu_h=u_{hg}$, $u_g{}^*=u_{g^{-1}}$. $\mathcal{H}$ *is generated by* $\mathcal{A}$ *and* $\{u_g\}$, $g\in\mathfrak{G}$. *For any function,* $a(x)$, $u_g\xi^au_g{}^*=\xi^b$, *where* $b(x)=a(xg^{-1})$.

3. The group of automorphisms leaving each element $\mathcal{A}$ fixed. If $S\in\mathfrak{S}$, then S restricted to $\mathcal{A}$ is an automorphism of the abelian H-system $\mathcal{A}$ and is induced by a measure preserving transformation S' on $(X,\boldsymbol{F},\mu)$. If f is the characteristic function of the set F, and fS' of FS' then $S^{-1}(\xi^f)=\xi^{fS'}$. The mapping $\phi:S\to S'$ is a homomorphism of $\mathfrak{S}$ into the group $\mathfrak{M}$ of all measure preserving transformations on $(X,\boldsymbol{F},\mu)$ for: $(TS)^{-1}(\xi^f)=S^{-1}(\xi^{fT'})=\xi^{fT'S'}$. We denote the image of ϕ by $\mathfrak{S}'$ and the kernel of ϕ by $\mathfrak{K}$. $S\in\mathfrak{K}$ if and only if S' is the identity transformation, if and only if $S(\xi^a)=\xi^a$ for all functions $a(x)$. In this section we analyze $\mathfrak{K}$.

[1] More general H-systems with maximal abelian algebras $\mathcal{A}\ni\mathcal{L}_{\mathcal{A}}\cup\mathcal{R}_{\mathcal{A}}$ are maximal abelian in the set of all operators have been considered by Ambrose ([2], pp. 45-46), and will be the topic of investigation with the author in a forthcoming joint paper. The procedure in Section 5 of this paper was suggested by some general results in our joint paper.

3.1 THEOREM. *$S \varepsilon \mathfrak{R}$ if and only if $S \sim \{S_{g,h}\}$, where $S_{g,h} = 0$ if $g \neq h$ and $S_{g,g}$ = multiplication by functions $s_g(x)$ satisfying*

(i) $|s_g(x)| = 1$ a. e. (ii) $s_{hg}(x) = s_h(xg^{-1})s_g(x)$ a. e.

Proof. If $S \varepsilon \mathfrak{R}$, $S(\xi^a\eta) = S(\xi^a)S(\eta) = \xi^a S(\eta)$. Also $S(\eta\xi^a) = S(\eta)S(\xi^a) = S(\eta)\xi^a$ for any bounded measurable function $a(x)$. Hence $S \varepsilon (\mathcal{L}_{\mathfrak{a}} \cup \mathcal{R}_{\mathfrak{a}})'$. By 2.4, $\{S_{g,h}\}$ is diagonal and $S_{g,g}$ is multiplication by a function $s_g(x)$. Since S is unitary, $S^* = S^{-1}$ and therefore $S_{g,g}^* = S_{g,g}^{-1}$ implying $\bar{s}_g(x) = s_g(x)^{-1}$. This proves (i). As for (ii), $S(u_{gh}) = S(u_h u_g) = S(u_h)S(u_g)$ means $s_{gh}u_{gh} = s_h u_h s_g u_g = s_g u_h s_g u_h^* u_{gh}$. Since $u_h s_g u_h^* = \tilde{s}_g$ where $\tilde{s}_g(x) = s_g(xh^{-1})$ we get $s_{gh}(x) = s_h(x)s_g(xh^{-1})$.

Conversely, if S is a diagonal matrix of the given type satisfying (i), it is a unitary operator in $\mathfrak{H}$, leaving each element of $\mathfrak{a}$ fixed. (ii) implies $S(u_g u_h) = S(u_g)S(u_h)$ and moreover $S(\xi^a u_g) = \xi^a S(u_g) = S(\xi^a)S(u_g)$. Hence S is an automorphism on $\mathfrak{B}$ and on all of $\mathfrak{H}$ because it is unitary.

3.2 THEOREM.[2] *Let $\mathfrak{J}$ be the set of all inner automorphisms of $\mathfrak{H}$. Then $\mathfrak{J} \cap \mathfrak{R} = [S \varepsilon \mathfrak{R}; s_g(x) = a(x)a(xg^{-1})$ for some $a(x)$ a measurable function of absolute value 1].*

Proof. If $S \varepsilon \mathfrak{J}$, $S(\eta) = \tau\eta\tau^*$ for some unitary $\tau \varepsilon \mathfrak{H}$. If $S \varepsilon \mathfrak{R}$ also, τ commutes with $\mathfrak{a}$ and hence lies in $\mathfrak{a}$. Thus $\tau = \xi^a$ and so $|a(x)| = 1$, $x \varepsilon X$. Also $S(u_g) = s_g u_g = \xi^a u_g \xi^{\bar{a}} = a(x)a(xg^{-1})u_g$.

3.3 THEOREM. *$\mathfrak{S}$ is a semidirect product of $\mathfrak{R}$ and a subgroup $\mathfrak{S}_1$ consisting of all $S_1 \varepsilon \mathfrak{S}$ satisfying the condition P: S_1 send u_g into $\tau_g \ni \tau_g(h, x)$ always consist of characteristic functions of sets.*

Proof. If $S \varepsilon \mathfrak{S}$,

$$\mathfrak{a} = S(\mathfrak{a}) = S(u_g \mathfrak{a} u_{g^{-1}}) = S(u_g)S(\mathfrak{a})S(u_g)^{-1} = S(u_g)\mathfrak{a}S(u_g)^{-1}.$$

Also $S(u_g)$ is unitary since S preserves adjoints. Hence $S(u_g)$ is a unitary element whose corresponding inner automorphism leaves $\mathfrak{a}$ invariant. By 2.3, $S(u_g) = \xi^{a_g}\tau_g$, a_g and τ_g satisfying the conditions of 2.3. Next note that

$$a_{hg}\tau_{hg} = S(u_{hg}) = S(u_g u_h) = a_g\tau_g a_h\tau_h = a_g(\tau_g a_h \tau_g^{-1})\tau_g\tau_h = b\tau_g\tau_h$$

[2] The theorems above can most neatly be described in terms of the cohomology theory of groups. For details, see [4]. Let $\mathfrak{C}$ denote the group of all measurable functions of absolute value 1 on X. The group $\mathfrak{G}$ acts on $\mathfrak{C}$ by virtue of its action on X, i.e., if $c(x) \varepsilon \mathfrak{C}$, $c_g(x) = c(xg^{-1})$. In terms of this action $Z_0 = H_0$ = circle group because $\mathfrak{G}$ acts ergodically on X and the constants are the only invariant elements $Z_1 = \mathfrak{R}$, $B_1 = \mathfrak{J} \cap \mathfrak{R}$ and $H_1 = \mathfrak{R}/\mathfrak{J} \cap \mathfrak{R}$ are the statements (3.1) and (3.2).

where $b(x) = a_g(x)\tilde{a}_h(x)$ and $\tilde{a}_h(x)$ is the image of $a_h(x)$ under the automorphism of $\mathfrak{A}$ due to τ_g. The uniqueness of the decomposition in 2.3 will show that $\tau_{hg} = \tau_g\tau_h$ if we can show that $\tau_g\tau_h(k, x)$ is the characteristic function of some set F. Suppose $\tau_g(k, x) = e_k(x)$ and $\tau_h(k, x) = f_k(x)$, where $e_h(x)$ and $f_k(x)$ are characteristic functions of the sets $E_k{}^{\tau_g}$ and $E_k{}^{\tau_h}$, the notation being that of 2.3. Then

$$\tau_g\tau_h(k, x) = \sum_{l \varepsilon \mathfrak{G}} \tau_g(l, x)\tau_h(kl^{-1}, xl^{-1}) = \sum_l e_l(x) f_{kl^{-1}}(xl^{-1})$$

which equals the characteristic function of the set $\bigcup_{l \varepsilon \mathfrak{G}} E_l{}^{\tau_g} \cap E_{kl^{-1}}{}^{\tau_h} l = F$ because $E_l{}^{\tau_g}$ are disjoint.

Let S_1 be the following operator on $\mathfrak{H}$: $(S_1\eta)(g, x) = \sum_g S(\xi^{\eta_g})\tau_g$ where $\eta_g(x) = \eta(g, x)$. In other words $\eta = \sum_g \xi^{\eta_g} u_g$ and S_1 has the same effect on $\mathfrak{A}$ as S does, but sends u_g into τ_g. We claim that S_1 is an automorphism of $\mathfrak{H}$. For, if $g \neq h$,

$$0 = (\mathfrak{A}u_g, \mathfrak{A}u_h) = (S(\mathfrak{A}u_g), S(\mathfrak{A}u_h)) = (S(\mathfrak{A})S(u_g), S(\mathfrak{A})S(u_h))$$
$$= (\mathfrak{A}\xi^{a_g}\tau_g, \mathfrak{A}\xi^{a_h}\tau_h) = (\mathfrak{A}\tau_g, \mathfrak{A}\tau_h).$$

Thus the elements in the sum for $S_1(\eta)$ are orthogonal and

$$(S_1\eta, S_1\nu) = \sum_g (S(\xi^{\eta_g})\tau_g, S(\xi^{\nu_g}\tau_g) = \sum_g (S(\xi^{\eta_g}), S(\xi^{\nu_g}))$$
$$= \sum_g (\xi^{\eta_g}, \xi^{\nu_g}) = (\eta, \nu)$$

i.e., S_1 is unitary.

S_1 preserves multiplication:

$$S_1(\xi^a u_g \xi^b u_h) = S_1(\xi^a u_g \xi^b u_{g^{-1}} u_{hg}) = S(\xi^a u_g \xi^b u_{g^{-1}})\tau_{hg}$$
$$= S(\xi^a)\xi^{a_g}(\tau_g S(\xi^b)\tau_{g^{-1}})\xi^{\bar{a}_g}\tau_g\tau_h = S(\xi^a)\tau_g S(\xi^b)\tau_h = S_1(\xi^a u_g) S_1(\xi^b u_h).$$

Since elements of the form $\xi^a u_g$ generate $\mathfrak{H}$, and since S_1 is a unitary operator, S_1 preserves multiplication. To show S_1 preserves adjoints, it suffices to show it does so on a set of generators. It does for $\mathfrak{A}$, since S does. It does on u_g, $g \varepsilon \mathfrak{G}$ for it preserves inverses.

We complete the proof by showing that $\mathfrak{S}_1$ is indeed a group. Suppose S_1 and $T_1 \varepsilon \mathfrak{S}_1$ and $S_1 u_g = \tau_g$ where $\tau_g(h, x) = e_h{}^g(x)$ the characteristic function of the set $E_h{}^g$. Similarly, $T_1 u_g = \nu_g$ where $\nu_g(h, x) = f_h{}^g(x)$, the characteristic function of the set $F_h{}^g$. Then

$$T_1 S_1(u_g) = T_1(\tau_g) = T_1(\sum_h e_h{}^g u_h) = \sum_h T_1(e_h{}^g)\nu_h$$
$$= \sum_{k,h} T_1(e_h{}^g) f_k{}^h u_k = \sum_k (\sum_h \bar{e}_h{}^g f_k{}^h) u_k$$

where $T_1(e_h{}^g) = \tilde{e}_h{}^g$; and $\tilde{e}_h{}^g$ are characteristic functions of sets $\tilde{E}_h{}^g$ which are disjoint over the index h for each $g \varepsilon \mathfrak{G}$ because T_1 is an automorphism and the $E_h{}^g$ enjoy this property also. We must show that $\sum_h \tilde{e}_h{}^g f_k{}^h$ is a characteristic function for each $g, k \varepsilon \mathfrak{G}$. In fact it is the characteristic function of the set $\bigcup_h (\tilde{E}_h{}^g \cap F_k{}^h)$ since the $\tilde{E}_h{}^g$ are disjoint for fixed $g \varepsilon \mathfrak{G}$.

3.4 Corollary. *Let* $\mathfrak{J}_{\mathfrak{K}} = \mathfrak{K} \cap \mathfrak{J}$ *and* $\mathfrak{J}_{\mathfrak{S}_1} = \mathfrak{J} \cap \mathfrak{S}_1$. *Then* $\mathfrak{S}/\mathfrak{J}$ *is the semidirect product of two groups* $\bar{\mathfrak{K}}$ *and* $\bar{\mathfrak{S}}_1$ *isomorphic respectively to* $\mathfrak{K}/\mathfrak{J}_{\mathfrak{K}}$ *and* $\mathfrak{S}_1/\mathfrak{J}_{\mathfrak{S}_1}$.

Proof. 2.3 shows that $\mathfrak{J}$ is the semidirect product of $\mathfrak{J}_{\mathfrak{K}}$ and $\mathfrak{J}_{\mathfrak{S}_1}$. Let $\bar{\mathfrak{K}}$ be the image of $\mathfrak{K}$ in $\mathfrak{S}/\mathfrak{J}$ and $\bar{\mathfrak{S}}_1$ the image of $\mathfrak{S}_1$. Then $\bar{\mathfrak{K}}$ is normal and $\bar{\mathfrak{K}} \cap \bar{\mathfrak{S}}_1$ is the identity element of $\mathfrak{S}/\mathfrak{J}$. For if $K\mathfrak{J} = S_1\mathfrak{J}$, then there exists a $J \varepsilon \mathfrak{J} \ni J = J_1 J_2{}^{-1}$, $J_1 \varepsilon \mathfrak{J}_{\mathfrak{K}}$ and $J_2 \varepsilon \mathfrak{J}_{\mathfrak{S}_1}$, and $KJ_1 = S_1 J_2$. But $KJ_1 \varepsilon \mathfrak{S}_1$ and $S_1 J_2 \varepsilon \mathfrak{S}_1$ so that $KJ_1 = I$; $K \varepsilon \mathfrak{J}$; $K\mathfrak{J} = \mathfrak{J}$. We have shown that $\mathfrak{S}/\mathfrak{J}$ is the semidirect product of $\bar{\mathfrak{K}}$ and $\bar{\mathfrak{S}}_1$. But $\bar{\mathfrak{K}} = \mathfrak{K} \cdot \mathfrak{J}/\mathfrak{J} \cong \mathfrak{K}/\mathfrak{J}_{\mathfrak{K}}$ by the first isomorphism theorem; similarly $\bar{\mathfrak{S}}_1 = \mathfrak{S} \cdot \mathfrak{J}/\mathfrak{J} \cong \mathfrak{S}_1/\mathfrak{J}_{\mathfrak{S}_1}$.

4. Some examples.

4.1 Lemma. *Suppose* $\mathfrak{G}$ *is a cyclic group with generator* g. *Let* $\mathfrak{Z} = [$*the group of all measurable functions on* X *with absolute value* 1 *with pointwise multiplication*$]$ *and let* $\mathfrak{Y} = [$*all* $a(x) \varepsilon \mathfrak{Z}$; $a(x) = b(xg^{-1})\bar{b}(x)$ *for some* $b(x) \varepsilon \mathfrak{Z}]$. *Then* $\mathfrak{K} \cong \mathfrak{Z}$ *and* $\mathfrak{J}_{\mathfrak{K}} \cong \mathfrak{Y}$.

Proof. Since $\mathfrak{G}$ is ergodic, $\mathfrak{G}$ is infinite cyclic. By 3.1, $\mathfrak{K}$ is isomorphic with the set of all mappings of $\mathfrak{G}$ into $\mathfrak{Z} \ni s_{hk}(x) = s_h(xk^{-1})s_k(x)$, $h, k \varepsilon \mathfrak{G}$, the mapping given by $g \to s_g(x)$. Let $s_n(x) = s_{g^n}(x)$, $n = 0, +1, \cdots$. The map is then completely determined by $s_1(x)$ for $s_{n+1}(x) = s_n(xg^{-1})s_1(x)$ which means $s_{n+1}(x) = \prod_{m=0}^{n} s_1(xg^{-m})$. Conversely, if $s \varepsilon \mathfrak{Z}$, let $s_{n+1}(x) = \prod_{m=0}^{n} s(xg^{-m})$ and we must show that $g^n \to s_n(x)$ will satisfy $s_m(xg^{-m})s_n(x) = s_{n+m}(x)$. By substitution $s_m(xg^{-n})s_n(x) = \prod_{i=0}^{m} s(xg^{-i}g^{-n}) \prod_{j=0}^{n} s(xg^{-j}) = \prod_{i=0}^{m+n} s(xg^{-i}) = s_{n+m}(x)$. This is a typical cohomology argument. By 3.2 and the above, $\mathfrak{J}_{\mathfrak{S}} \cong \mathfrak{Y}$.

Let $(X, \boldsymbol{F}, \mu)$ be the measure space of a compact separable abelian group with μ Haar measure. Let g be a group element of $X \ni \{g^n\}$, $n = 0, \pm 1, \pm 2, \cdots$ is dense in X. Then right multiplication by g^{-1} is an ergodic transformation. ([6], p. 348; this paper also shows that we could use any $(X, \boldsymbol{F}, \mu)$ and g, providing g is an ergodic transformation with pure point spectrum.)

4.2 THEOREM. *Let $\chi_0 \varepsilon X^*$, the character group of X. If χ_0 is of infinite order, then $\chi_0 \not\varepsilon \mathfrak{Y}$, and therefore gives rise to an outer automorphism of $\mathfrak{A}$. In particular, if X is connected, $\mathfrak{K}/\mathfrak{J}$ contains a subgroup isomorphic to X^*.*

Proof. Suppose there exists $b(x) \varepsilon Z \ni b(x)\chi_0(x) = b(xg^{-1})$. Let b have the Fourier series L_2 expansion $\sum_{\chi \varepsilon X} \alpha_\chi \chi$. The previous equality shows $\sum_\chi \alpha_\chi \chi\chi_0 = \sum_\chi \alpha_\chi \bar{\chi}(g)\chi = \sum_\chi \alpha_{\chi\chi_0}\bar{\chi}\bar{\chi}_0(g)\chi\chi_0$. By the uniqueness of the expansion, $\alpha_\chi = \alpha_{\chi\chi_0}\chi\chi_0(g)$ and $|\alpha_\chi| = |\alpha_{\chi\chi_0}| = |\alpha_{\chi\chi_0^2}| = \cdots = |\alpha_{\chi\chi_0^n}|$. If χ_0 is infinite cyclic, this last shows that $\sum_\chi |\alpha_\chi|^2 = \infty$ unless all $\alpha_\chi = 0$. Since b is bounded measurable and not the 0 function, we have a contradiction. Hence $\chi_0 \not\varepsilon \mathfrak{Y}$.

If X is connected, no $\chi_0 \varepsilon X^*$, but the identity has finite order for the range would then be disconnected. Since multiplication of characters is the same as pointwise multiplication, $X^* \subseteqq \mathfrak{Z}$ and $X^* \cap \mathfrak{Y} =$ identity. Hence X is naturally isomorphic to a subgroup of $\mathfrak{Z}/\mathfrak{Y} \cong \mathfrak{K}/\mathfrak{J}_{\mathfrak{K}}$. The example just given exhibits lots of outer automorphisms.

4.3 THEOREM. *Let $X =$ circle group, $\mu =$ Haar measure, g an irrational rotation. Then $a(x) = (e^{ix} - p)/(1 - e^{ix}\bar{p})$ is in $\mathfrak{Z}$ but not in $\mathfrak{Y}$, for all $|p| < 1$.*

Proof. Since $|e^{ix} - p/1 - e^{ix}\bar{p}| = |e^{ix}||1 - e^{-ix}p|/|1 - e^{ix}\bar{p}| = 1$, $a(x) \varepsilon \mathfrak{Z}$. Suppose there exists a function $b(x) \ni a(x)b(x) = b(x - g)$. Then $b(x)(e^{ix} - p) = (1 - e^{ix}\bar{p})b(x - g)$. If $b(x) \sim \sum_n \alpha_n e^{inx}$ we get

$$\sum_n (\alpha_n e^{i(n+1)x} + \bar{p}\alpha_n e^{-ing} e^{inx}) = \sum_n (\alpha_n e^{-ing} e^{inx} + p\alpha_n e^{inx})$$

or

$$\sum_n \alpha_{n-1}(1 + \bar{p}e^{-i(n-1)g})e^{inx} = \sum_n \alpha_n(e^{-ing} + p)e^{inx}.$$

By the uniqueness of the expansion,

$$|\alpha_n| = |\alpha_{n-1}||1 + \bar{p}e^{-i(n-1)g}|/|p + e^{-ing}| = |\alpha_{n-1}||w^{n-1} + p|/|w^n + p|$$

where $w = e^{-ig}$. An easy computation shows this recursion formula gives $|\alpha_{n+k}| = |\alpha_{n-1}||w^{n-1} + p|/|w^{n+k} + p|$. Since the factor

$$|w^{n-1} + p|/|w^{n+k} + p| > (1 - |p|)/2 > 0,$$

$$\sum_{k=-1}^{\infty} |\alpha_{n+k}|^2 \geqq (1 - |p|)^2/2^2 \sum_{k=-1}^{\infty} |\alpha_{n-1}|^2 = \infty$$

so that, as before $b(x) = 0$, a contradiction. (By analogous means, one can exhibit many functions in $\mathfrak{Z}$ not in $\mathfrak{Y}$. However, the author has not succeeded in describing $\mathfrak{Z}/\mathfrak{Y}$ or those functions in $\mathfrak{Z}$ but not in $\mathfrak{Y}$ in any reasonable fashion.)

Our next example will be used for another purpose. It is well known [9] that, for the factor of all bounded operators, the double commutator of any weakly closed self-adjoint subalgebra is the algebra itself. In [5], it is shown that for any finite factor, there always exists a subfactor whose double relative commutator (relative to the factor) is larger than the subfactor. R. V. Kadison conjectured that perhaps a Galois-like theorem was true. Namely, if $\mathcal{H}_1$ is a subfactor of $\mathcal{H}$, and $\mathfrak{S}_{\mathcal{H}_1}$ the group of all automorphisms leaving each element of $\mathcal{H}_1$ fixed, then the set of all elements left fixed by $\mathfrak{S}_{\mathcal{H}_1}$ is exactly $\mathcal{H}_1$. (The failure of the double commutator theorem amounts to saying that using inner automorphisms would not suffice.) The author conjectured that perhaps some "reasonable" topology exists, rather than the weak one, for which the theorem would hold. Neither is the case as we now show.

4.5 Lemma. *Let $\mathfrak{G}_1$ be a subgroup of $\mathfrak{G}$, and let $\mathcal{H}_1 = [\eta \in \mathcal{H}; \eta(g, x) = 0$ if $g \notin \mathfrak{G}_1]$. $\mathcal{H}_1$ is a weakly closed subalgebra of $\mathcal{H}$ containing $\mathcal{A}$ and is a factor if and only if $\mathfrak{G}_1$ is ergodic on X. Let $\mathfrak{K}_1 = [S \in \mathfrak{K}; S(\eta) = \eta$ for all $\eta \in \mathcal{H}_1]$. Then $S \sim \{s_g(x)\} \in \mathfrak{K}_1$ if and only if $s_g(x) = 1$ a. e. for all $g \in \mathfrak{G}_1$.*

Proof. The map $\eta \to \eta(g, x) = \eta_g(x)$ is a continuous mapping from $\mathcal{H}$ to $\mathcal{L}_2(X, \boldsymbol{F}, \mu)$ and hence $\mathcal{H}_1$ is strongly and weakly closed. The other statements are easily verified.

4.6 Theorem. *If $\mathfrak{G}_1$ is a normal subgroup of $\mathfrak{G}$ such that $\mathfrak{G}/\mathfrak{G}_1$ is not abelian, and if $\mathfrak{G}_1$ acts ergodically on X, then the set of all elements in $\mathcal{H}$ left fixed by $\mathfrak{K}_1$ is strictly larger than $\mathcal{H}_1$. In particular, if $\mathfrak{G}/\mathfrak{G}_1$ equals its commutator, $\mathfrak{K}_1$ consists of the identity alone.*

Proof. We first show that $\mathfrak{K}_1$, as a group, is isomorphic to $(\mathfrak{G}/\mathfrak{G}_1)^*$, the homomorphisms of $\mathfrak{G}/\mathfrak{G}_1$ into the circle group. If $S \sim \{s_g(x)\} \in \mathfrak{K}_1$, then it gives rise to the following mapping χ_S of $\mathfrak{G}/\mathfrak{G}_1$ into $\mathfrak{Z}$. For any coset $\mathfrak{G}_1 g$, we let $\chi_S(\mathfrak{G}_1 g) = s_g(x)$. This is independent of the representative of the coset since $s_{g_1 g}(x) = s_{g_1}(xg^{-1}) s_g(x) = s_g(x)$ because $s_{g_1}(x) = 1$ a. e., $g_1 \in \mathfrak{G}_1$. Since $\mathfrak{G}_1$ is normal, $s_g(x) = s_{g_1 g}(x) = s_{g g_1}(x) = s_g(x g_1^{-1}) s_{g_1}(x) = s_g(x g_1^{-1})$ i. e., $s_g(x)$ is invariant under all $g_1 \in \mathfrak{G}_1$. But $\mathfrak{G}_1$ is ergodic so that $s_g(x)$ is a scalar of absolute value 1. Hence χ_S maps $\mathfrak{G}/\mathfrak{G}_1$ into the circle group. Finally it is a homomorphism; for $\chi_S(\mathfrak{G}_1 g \cdot \mathfrak{G}_1 h) = \chi_S(\mathfrak{G}_1 gh) = s_{gh}(x)$

$= s_g(xh^{-1})s_h(x) = s_g(x)s_h(x) = \chi_S(\mathfrak{G}_1 g)\chi_S(\mathfrak{G}_1 h)$. Hence χ_S lies in $(\mathfrak{G}/\mathfrak{G}_1)^*$. If χ_S is the identity element, then $s_g(x) = 1$ a. e. and $S = I$. The map $\chi : S \to \chi_S$ is a homomorphism because $ST \sim \{s_g(x)t_g(x)\}$. χ is onto for, given any character χ_0, define $S_0 = s_g{}^0(x)$ where $s_g{}^0(x) = \chi_0(\mathfrak{G}_1 g)$ and then $\chi(S_0)$ will equal χ_0. (This is a relative cohomology argument.)

Since the circle group is abelian, $(\mathfrak{G}/\mathfrak{G}_1)^* \cong (\mathfrak{G}/\mathfrak{G}_1/[\ ])^*$ where $[\ ]$ denotes the commutator subgroup of $\mathfrak{G}/\mathfrak{G}_1$. If $[\ ] = \mathfrak{G}/\mathfrak{G}_1$, then $(\mathfrak{G}/\mathfrak{G}_1)^* = (e)$ and $\mathfrak{R}_1$ consists of the identity alone. More generally, if $\mathfrak{G}/\mathfrak{G}_1$ is not abelian, it has a commutator. Suppose $g \in \mathfrak{G}$ is an element $\ni \mathfrak{G}_1 g$ is a commutator and $\mathfrak{G}_1 g \neq \mathfrak{G}_1$. If $s \in \mathfrak{R}_1$, then $\chi_S(\mathfrak{G}_1 g) \equiv 1 = s_g(x)$. Therefore $S(u_g) = \xi^{s_g} u_g = u_g$, i. e. u_g is left fixed by S. But this $g \notin \mathfrak{G}_1$ and hence $u_g \notin \mathcal{H}_1$.

We add that if by a "reasonable topology" we mean one such that the projection map $\eta \to \eta_g(x)$ is continuous from $\mathcal{H}$ to $\mathcal{L}_2(X, \boldsymbol{F}, \mu)$, then $\mathcal{H}_1$ is closed in this topology and still does not satisfy the Galois theorem.

For a specific example of the situation in 4. 6, consider the measure space $(X, \boldsymbol{F}, \mu)$ where X is the circle again and μ Haar measure. $\mathfrak{G}$ is the group generated by two irrational rotations α and β not rationally connected, together with the reflection $x \to -x$. $\mathfrak{G}$ is isomorphic to the set of triples $\{(n\alpha, m\beta, \pm 1)\}$, $n, m = 0, \pm 1, \pm 2, \cdots$ in which multiplication is given by

$$(n\alpha, m\beta, -1)(n_1\alpha, m_1\beta, \pm 1) = ((n - n_1)\alpha, (m - m_1)\beta, \mp 1);$$

$$(n\alpha, m\beta, +1)(n_1\alpha, m_1\beta, \pm 1) = ((n + n_1)\alpha, (m + m_1)\beta, \pm 1).$$

The isomorphism can be set up by the condition that the triple $(n\alpha, m\beta, -1)$ acts on x by $x(n\alpha, m\beta, -1) = -x - n\alpha - m\beta$. One can now check the conditions 1. 2 and 1. 3, to be assured that we do get a finite factor. Let $\mathfrak{G}_1 = \{(n\alpha, 0, +1)\}$, $n = 0, \pm 1, \cdots$. $\mathfrak{G}_1$ is normal and moreover, $\mathfrak{G}/\mathfrak{G}_1 \cong \{(0, m\beta, \pm 1)\}$, $m = 0, \pm 1, \pm 2, \cdots$, which is not abelian.

Finally, is Section 5, the normalizer $\mathfrak{N}$ of $\mathfrak{G}$, as a subgroup of all measure preserving transformations takes on importance and we want to compute $\mathfrak{N}$ in the special case where $\mathfrak{G} = \{g^n\}$ $n = 0, \pm 1, \pm 2, \cdots$, and g is an irrational rotation on the circle. If $N \in \mathfrak{N}$ and $NgN^{-1} = g$ then by ([6], Cor. 2, p. 347), N is a rotation. If $NgN^{-1} = g^{-1}$ then $NRg = gNR$ where R is the reflection $x \to -x$. Thus $\mathfrak{N}$ is the semidirect product of the group of all rotations with the group of order two with generator $\mathfrak{R}$.

5. The subgroup $\mathfrak{S}_1$. Since $\mathfrak{S}$ is a semidirect product of $\mathfrak{R}$ and $\mathfrak{S}_1$, and since $\mathfrak{S}/\mathfrak{R} \cong \mathfrak{S}_1'$ a subgroup of all measure preserving transformations, $\mathfrak{S}_1 \cong \mathfrak{S}_1'$ and we can view $\mathfrak{S}_1$ as a group of measure preserving transformations

(m.p.t.). In this section we analyze this group, in particular we study its relation to the original group $\mathfrak{G}$.

5.1 THEOREM. *A necessary and sufficient condition that a m.p.t. S' stem from an automorphism $S \varepsilon \mathfrak{S}_1$ is that there exist sets $E_h{}^g \varepsilon \mathbf{F}, g, h \varepsilon \mathfrak{G}$ such that*

(i) $\mu(E_h{}^g \cap E_k{}^g) = 0$ *for* $h \neq k$.

(ii) $\mu(\bigcup_h E_h{}^g) = 1$.

(iii) *On* $E_h{}^g S'$, $(S')^{-1}h^{-1}S' = g^{-1}$.

Proof. This theorem says that the m.p.t. S' will lead to an automorphism if and only if for each $g \varepsilon \mathfrak{G}$, X can be decomposed into disjoint sets $E_h{}^g S'$ on which $(S')^{-1}h^{-1}S'$ looks like g^{-1}.

Now if $S \varepsilon \mathfrak{S}_1$, S induces a measure preserving transformation S' on $X \ni S^{-1}(\xi^e) = \xi^f$ where e and f are the characteristic functions of the sets E and ES' respectively. As briefly described at the beginning of Section 3, S' induces an automorphism on the H system $L_2(X, \mathbf{F}, \mu)$ which sends $a \to a_{S'}$, and which agrees with the restriction of S to $\mathfrak{A}$. So if $a(x) \varepsilon \mathfrak{A}$, $S(a) = a_{S'}$. (If S' were a point transformation, $a_{S'}(x) = a(xS')$.)

As before let $S(u_g) = \tau_g$ so that $\tau_g(h, x) = e_h{}^g$, the characteristic functions of the sets $E_h{}^g$. By 2.2, the $E_h{}^g$ satisfy (i). We now show they satisfy (ii). Let v be a unitary in $\mathfrak{H} \ni v\mathfrak{A}v^{-1} = \mathfrak{A}$. Let $J(v)$ be the inner automorphism on $\mathfrak{H}$ due to v. Then $J(v) \varepsilon \mathfrak{S}$. It is easy to check that $J(u_g) \varepsilon \mathfrak{S}_1$ and $(J(u_g))' = g^{-1}$. Since

$$(SJ(u_g))(\mathfrak{A}) = S(u_g \mathfrak{A} u_g{}^*) = \tau_g S(\mathfrak{A})\tau_g{}^* = (J(\tau_g)S)(\mathfrak{A}),$$

we see that $S'g^{-1}(S')^{-1} = (J(\tau_g))'$. By 2.3, $(J(\tau_g))'$ looks like this: If $x \varepsilon E_h{}^g h^{-1}$ then $x(J(\tau_g))' = xh$, i.e., $E_h{}^g h^{-1}S'g^{-1}(S')^{-1} = E_h{}^g h^{-1}(J(\tau_g))' = E_h{}^g$, pointwise which was to be proved.

Conversely, suppose S' satisfies the conditions of the theorem, relative to the sets $E_h{}^g$. S', by virtue of being m.p.t., is already an automorphism of $\mathfrak{A}$ by $S(\xi^a) = \xi^{a_{S'}}$. We extend S as follows: $S(u_g) = \tau_g$, where $\tau_g(h, x) = e_h{}^g(x)$; $S(\xi^a u_g) = S(\xi^a)\tau_g$ and now extend S to be linear on finite linear combinations of elements of the form $\xi^a u_g$. We show S is an automorphism. First, $\tau_g\tau_h = \tau_{hg}$. For $\tau_g\tau_h(k, x) = \sum_l \tau_g(l, x)\tau_h(kl^{-1}, xl^{-1}) = \sum_{l_1} \tau_g(l_1{}^{-1}k, x)\tau_h(l_1, xk^{-1}l_1) = f_k(x)$ where $F_k = \bigcup_l E_{l^{-1}k}{}^g \cap E_l{}^h l^{-1}k$ since $E_{l^{-1}k}{}^g$ are disjoint for distinct l. If $x \varepsilon F_k$, then for some l, $x \varepsilon E_{l^{-1}k}{}^g$ and $xk^{-1}l \varepsilon E_l{}^h$ so that $xk^{-1}lS' = xS'g^{-1}$ and $xk^{-1}ll^{-1}S' = xk^{-1}lS'h^{-1}$. Therefore $xk^{-1}S' = xS'g^{-1}h^{-1}$ and $x \varepsilon E_k{}^{hg}$. So far we

have shown that $F_k \subseteqq E_k{}^{hg}$. On the other hand, by changing variables back again $F_k = \bigcup_l (E_l{}^g \cap E_{kl^{-1}}{}^h l)$ and $\bigcup_k F_k = \bigcup_l (E_l{}^g \cap (\bigcup_k E_{kl^{-1}}{}^h) l) = X$. Hence

$$0 = \mu(X - \bigcup_k F_k) = \mu(\bigcup_k E_k{}^{hg} - \bigcup_k F_k)$$
$$= \mu(\bigcup_k (E_k{}^{hg} - F_k)) = \sum_k \mu(E_k{}^{hg} - F_k)$$

and $f_k = e_k{}^{hg}$ a. e. This proves

$$\tau_g \tau_h = \tau_{hg} \text{ and } S(u_g u_h) = \tau_{hg} = \tau_g \tau_h = S(u_g) S(u_h).$$

By 2. 2, the τ_g are unitary and $(J(\tau_g))(\mathfrak{A}) \subseteqq \mathfrak{A}$ since $E_{h_1}{}^g h_1{}^{-1} \cap E_{h_2}{}^g h_2{}^{-1}$ is empty if $h_1 \neq h_2$; that is, by (iii), on $E_{h_i}{}^g h_i{}^{-1}$, $h_i S' g (S')^{-1}$ acts like the identity, $(i = 1, 2)$ so that on the intersection h_1 acts like h_2.

We now show that $S(\xi^a u_g \xi^b u_h) = S(\xi^a u_g) S(\xi^b u_h)$. Since

$$S(\xi^a u_g \xi^b u_h) = S(\xi^a (u_g \xi^b u_g{}^*) u_{hg})$$
$$= S(\xi^a) S(u_g \xi^b u_g{}^*) \tau_g \tau_h = S(\xi^a) \tau_g \tau_g{}^{-1} S(u_g \xi^b u_g{}^{-1}) \tau_g \tau_h$$

it suffices to show that $S(u_g \xi^b u_g{}^*) = \tau_g S(\xi^b) \tau_g{}^{-1}$. But $S(u_g \xi^b u_g{}^*) = \xi^c$ where $c(x) = b(xg(S')^{-1})$, while $\tau_g S(\xi^b) \tau_g{}^* = \xi^d$ where $d(x) = b(xg(S')^{-1}(J(\tau_g))')$. We must show that the m.p.t. $S'g$ equals $(J(\tau_g))'S'$. But we have already seen in 2. 3, that if $x \in E_h{}^g h^{-1}$, then $x(J(\tau_g))' = xh$. Condition (iii) says that if $x \in E_h{}^g h^{-1}$, then $xS' = xhS'g^{-1} = x(J(\tau_g))'S'g^{-1}$. Hence on $E_h{}^g h^{-1}$, $S'g = (J(\tau_g))'S'$. Since $\bigcup_h (E_h{}^g h^{-1}) = X$, $S'g = (J(\tau_g))'S'$ a. e., which was to be proved.

By linearity, then, we have shown that S preserves addition and multiplication on a dense subset of S. It also preserves adjoints since $S(u_g{}^*) = S(u_{g^{-1}}) = \tau_{g^{-1}} = (\tau_g)^* = (S(u_g))^*$ and it preserves complex conjugate on $L_2(X, \boldsymbol{F}, \mu) = \mathfrak{A}$. The extension to all of $\mathfrak{H}$ can be made as soon as we show that S preserves inner products on linear combinations of $\xi^a u_g$. A direct computation shows that it suffices to prove that $(\mathfrak{A}\tau_g, \tau_h) = 0$ if $g \neq h$. But

$$(\xi^a \tau_g, \tau_h) = \sum_k (a(x) e_k{}^g, e_k{}^h) = \sum_k \int_{E_k{}^g \cap E_k{}^h} a(x) d\mu = 0$$

if $\mu(E_k{}^g \cap E_k{}^h) = 0$ when $g \neq h$. By (iii), on $E_k{}^g S'$, $(S')^{-1} k^{-1} S' = g^{-1}$ and on $E_k{}^h S'$, $(S')^{-1} k^{-1} S' = h^{-1}$ so that $g^{-1} = h^{-1}$ on

$$E_k{}^g S' \cap E_k{}^h S' = (E_k{}^g \cap E_k{}^h) S'.$$

Hence $\mu(E_k{}^g \cap E_k{}^h) = 0$.

The theorem just proved has an interesting geometric interpretation,[1]

which we are about to describe. No proofs will be given, since the proofs would amount to a reshuffling of the statements in the proof of 5. 1. We introduce a measure m on the product space $(X \times X, \boldsymbol{F} \times \boldsymbol{F})$ which will be concentrated on the graphs of g, $g \,\varepsilon\, \mathfrak{G}$, i. e., concentrated on the sets of the form $X^g = [(x, xg^{-1}), x \,\varepsilon\, X]$. For any $E \,\varepsilon\, \boldsymbol{F}$ let $E^g = [(x, xg^{-1}), x \,\varepsilon\, E]$. Then the measure m will be completely determined by the conditions that m be concentrated on X^g and $m(E^g) = \mu(E)$, i. e., the map $x \rightarrow (x, xg^{-1})$ is measure preserving into, for all $g \,\varepsilon\, \mathfrak{G}$.

There is a natural isometry of the Hilbert space $\mathfrak{H}$ onto $L_2(X \times X, \boldsymbol{F} \times \boldsymbol{F}, m)$ which is given by sending any $\eta \,\varepsilon\, \mathfrak{H}$ into the function η' on $X \times X$ where $\eta'(x, y) = 0$ if $y \neq xg^{-1}$ for some $g \,\varepsilon\, \mathfrak{G}$; and $\eta'(x, xg^{-1}) = \eta(g, x)$. (This is well defined, for by (1. 2), $(x, xg^{-1}) = (x, xh^{-1})$ only on an m-set of m-measure 0.) This isometry says little more than the fact that $\mathfrak{H}$ equals $\sum_{\mathfrak{G}} \oplus L_2(X, \boldsymbol{F}, \mu)$ as does $L_2(X \times X, \boldsymbol{F} \times \boldsymbol{F}, m)$. However, the important thing in this mapping is that multiplication in $\mathfrak{H}$ goes over to ordinary matrix multiplication in $L_2(X \times X, \boldsymbol{F} \times \boldsymbol{F}, m)$. By ordinary matrix multiplication, we mean $\eta'\tau'(x, y) = \sum_z \eta'(x, z)\tau'(z, y)$. We use the ordinary sum because, since $\mathfrak{G}$ is countable, there is at most a countable number of values z on which $\eta'(x, z) \neq 0$. (If $\mathfrak{G}$ were the group of order n generated by the cycle $(12 \cdots n)$ acting on the space X of n elements, the above description would lead to the algebra of all $n \times n$ matrices.)

To each m.p.t., S' on $(X, \boldsymbol{F}, \mu)$, we associate a transformation $S' \times S'$ on $(X \times X, \boldsymbol{F} \times \boldsymbol{F})$ which amounts to $(x, y)S' \times S' = (xS', yS')$ if S' were a point transformation. Then Theorem 5. 1 can be rephrased to say: *A necessary and sufficient condition a m.p.t. S' stem from an automorphism $S \,\varepsilon\, \mathfrak{S}_1$ is that $S' \times S'$ preserve the m-null sets of $(X \times X, \boldsymbol{F} \times \boldsymbol{F}, m)$. This is to be expected since the carrier of m carries all the algebraic structure of the H-system.* We leave the proof to the reader, but wish to point out that in this context,

$$\begin{aligned}(X^g)S' \times S' \cap X^h &= [(y, yh^{-1})\,;\, y(S')^{-1}g^{-1}S' = yh^{-1}]\\ &= [(y, yh^{-1})\,;\, y \,\varepsilon\, E_g{}^h S'].\end{aligned}$$

5. 2 THEOREM. *Let $\mathfrak{N}$ denote the normalizer of $\mathfrak{G}$ in the group of all m.p.t. Then $\mathfrak{N} \subseteq \mathfrak{S}$, and if $N' \,\varepsilon\, \mathfrak{N}$, then the associated $E_h{}^g = X$ if $h^{-1}N' = N'g^{-1}$ and $E_h{}^g$ is empty otherwise. If τ is a unitary $\ni J(\tau) \,\varepsilon\, \mathfrak{J}_{S_1}$ then $\tau(g, x) = f_g(x)$ and the corresponding*

$$E_h{}^g = \bigcup_k (F_{hk} \cap F_{kg}g^{-1})k^{-1} = \bigcup_l (F_l \cap F_{hlg^{-1}g})l^{-1}$$

where $f_g(x)$ is the characteristic function of F_g.

Proof. The first part of the theorem follows from the definition of normalizer. For the second statement, (2.3) says that if $x \varepsilon F_{g^{-1}g}$, then $x(J(\tau))' = xg^{-1}$. Suppose that $x \varepsilon F_{hk^{-1}k} \cap F_{k^{-1}g}g^{-1}k$. Then $xh^{-1} \varepsilon F_{hk^{-1}}hk^{-1}$ and $xh^{-1}(J(\tau))' = xh^{-1}hk^{-1} = xk^{-1}$; $x \varepsilon F_{k^{-1}g}(k^{-1}g)^{-1}$ and $x(J(\tau))' = xk^{-1}g$. Hence $xh^{-1}(J_\tau)' = x(J(\tau))'g^{-1}$ so that $x \varepsilon E_h{}^g$, i.e.,

$$F_h{}^g = \bigcup_k (F_{hk^{-1}} \cap F_{k^{-1}g}g^{-1})k \subseteqq E_h{}^g.$$

However,

$$\bigcup_h F_h{}^g = \bigcup_k (\bigcup_h F_{hk^{-1}} \cap F_{k^{-1}g}g^{-1})k = \bigcup_k F_{k^{-1}g}g^{-1}k = X,$$

so that $\mu(E_h{}^g - F_h{}^g) = 0$. The second form for $E_h{}^g$ can be obtained by making the change of variables from k to $l = gk$.

For a complete description of $\mathfrak{S}_1/\mathfrak{J}_{\mathfrak{S}_1}$, it would be nice to know a great deal about $\mathfrak{N} \cap \mathfrak{J}_{\mathfrak{S}_1}$ and $\mathfrak{N} \cup \mathfrak{J}_{\mathfrak{S}_1}$. We collect this information below.

5.3 LEMMA. $\mathfrak{G} \subseteqq \mathfrak{N} \cap \mathfrak{J}_{\mathfrak{S}_1}$. *Suppose* $T' = (J(\tau))' \varepsilon \mathfrak{N} \cap \mathfrak{J}_{\mathfrak{S}_1}$ *and* $\tau(g, x) = f_g(x)$ *as above. If* $\mu(F_l) > 0$, *the subgroup*

$$\mathfrak{G}_T{}^l = [g \varepsilon \mathfrak{G}; lgl^{-1} = T'g]$$

is of finite index r, *where* $r \leqq 1/\mu(F_l)$.

Proof. $(J(u_g))' = g^{-1}$ shows $\mathfrak{G} \subseteqq \mathfrak{N} \cap \mathfrak{J}_{\mathfrak{S}_1}$. If $T' = (J(\tau))'$ then by 5.2, the corresponding $E_h{}^g = \bigcup_l (F_l \cap F_{hlg^{-1}g})l^{-1}$. If in addition, $T' \varepsilon \mathfrak{N}$ then $E_h{}^g$ is empty unless $h = (T')^{-1}gT' = g'$. This means $F_l \cap F_{hlg^{-1}g}$ is empty unless $h = g'$ and for each l, $F_l = F_{g'lg^{-1}g}$ and therefore $m(F_l) = m(F_{g'lg^{-1}})$. If $g_1, \cdots, g_s$ lie in distinct left cosets of $\mathfrak{G}_T{}^l$, then $g_i'lg_i \neq g_j'lg_j$, $i \neq j$ and $i, j = 1, \cdots, s$. Therefore the sets $F_{g_i'lg_i}$ are disjoint. They have the same measure and yet $\mu(X) = 1$. Hence $s \leqq 1/\mu(F_l)$.

The lemma shows that for any $g \varepsilon \mathfrak{G}$, $g^n \varepsilon \mathfrak{G}_T{}^l$ for some $n \leqq r$. In particular if G has unique n-th roots, when they exist, (for example if G is free abelian) then $lg^nl^{-1} = (T')^{-1}g^nT'$ implies $lgl^{-1} = (T')^{-1}gT'$ for all $g \varepsilon \mathfrak{G}$, i.e. $\mathfrak{N} \cap \mathfrak{J}_{\mathfrak{S}_1} = \mathfrak{G}$. This is surely the case in the example discussed in 4.1. In this case, then, $\mathfrak{S}_1/\mathfrak{J}_{\mathfrak{S}_1} \cong \mathfrak{S}'_1/\mathfrak{J}'_{\mathfrak{S}_1}$ contains $\mathfrak{N} \cup \mathfrak{J}'_{\mathfrak{S}_1}/\mathfrak{J}'_{\mathfrak{S}_1}$ as a subgroup. By the first isomorphism theorem for groups, this last group is isomorphic to $\mathfrak{N}/\mathfrak{N} \cap \mathfrak{J}'_{\mathfrak{S}_1}$ which becomes $\mathfrak{N}/\mathfrak{G}$. At the end of Section 4, $\mathfrak{N}$ is computed for a special case, and we see that $\mathfrak{N}/\mathfrak{G}$ has many elements, i.e., that there are many outer automorphisms in $\mathfrak{S}_1$.

The author has been unable to decide the quesion: Is $\mathfrak{N} \cup \mathfrak{J}'_{\mathfrak{S}_1} = \mathfrak{S}'_1$? However the following lemma is relevant to this question.

5.4 LEMMA. *If* $S' \varepsilon \mathfrak{S}'_1$, $S' \sim \{E_h{}^g\}$ *and* $T' \varepsilon \mathfrak{S}'_1$, $T' \sim \{F_h{}^g\}$ *then* $S'T' = (ST)' \sim \{\bigcup_k E_h{}^k \cap (F_k{}^g(S')^{-1})\}$.

Proof. The notation in the lemma means that on $E_h{}^g S'$ the transformation $(S')^{-1}h^{-1}S' = g^{-1}$ and on $F_h{}^g T'$ the transformation $(T')^{-1}h^{-1}T' = g^{-1}$. If $x \varepsilon E_h{}^k$ and $x \varepsilon F_k{}^g(S')^{-1}$, then $xh^{-1}S' = xS'k^{-1}$. Also $xS' \varepsilon F_k{}^g$ so that $xS'k^{-1}T' = xS'T'g^{-1}$. A combination of these two equation gives $xh^{-1}S'T' = xS'T'g^{-1}$, so that $x \varepsilon G_h{}^g$ where $S'T' = (ST)' \sim \{G_h{}^g\}$. We have shown that $\bigcup_k (E_h{}^k \cap (F_k{}^g(S')^{-1})) \subseteq G_h{}^g$. These two sets are in fact equal; for

$$\bigcup_h \bigcup_k (E_h{}^k \cap (F_k{}^g(S')^{-1})) = \bigcup_k ((\bigcup_h E_h{}^k) \cap F_k{}^g(S')^{-1}) = \bigcup_k X \cap F_k{}^g(S')^{-1} = X.$$

If $S' = (J(\tau))' \varepsilon \mathfrak{J}'_{\mathfrak{S}_1}$ and $T' \varepsilon \mathfrak{N}$, then $F_k{}^g = X$ if $k = (T')^{-1}gT'$ and empty otherwise so that $G_h{}^g = E_h{}^k$, and by 5.2, $E_h{}^k = \bigcup_l (F_l \cap F_{hlk^{-1}k})l^{-1}$. To prove that $\mathfrak{N} \cup \mathfrak{J}'_{\mathfrak{S}_1} = \mathfrak{S}'_1$ then, one must show that given a collection of sets $\{G_h{}^g\}$ satisfying the conditions in (5.1), one can find a collection of sets $\{F_k\}$ satisfying (2.2) $\ni G_h{}^k = \bigcup_l (F_l \cap F_{hlk^{-1}k})l^{-1}$ for some $k \varepsilon G$ where k would equal $(T')^{-1}gT'$. We have been unable to prove this or find a counter-example, even in the simplest case discussed at the end of Section 4.

6. Concluding remarks. If the assumption of the ergodicity of $\mathfrak{G}$ is relaxed, the H-system obtained will no longer be simple. Nevertheless, it should be fairly clear to the expert that, with enough techniques, the constructions in this paper can still be carried through in that more general context. We have not done this; firstly, because it would obscure the basic ideas in the paper, and secondly, because the author is primarily interested in simple systems. The direct integral decomposition theory has been sufficiently well worked out so that almost all questions about general systems reduce to questions about simple ones.

However, there is a generalization of the Murray-von Neumann construction which we find more interesting. We can view the simple H-system $\mathcal{H}$ under discussion as having been obtained by taking a maximal abelian self adjoint algebra of all bounded operators on a Hilbert space (in our case $L_2(X, \boldsymbol{F}, \mu) = \mathcal{A}$) together with a countable group of unitaries leaving $\mathcal{A}$ invariant (in our case, the unitaries induced by the m.p.t.'s $g \varepsilon G$), and performing the original tensor product construction. Clearly $\mathcal{A}$ need not be so special. $\mathcal{A}$ could be any algebra, or equivalently, any H-system, and $\mathfrak{G}$ any countable group of automorphisms of $\mathcal{A}$. If enough conditions are put

on the action of $\mathfrak{G}$ on $\mathcal{A}$, the tensor product construction will give simple systems, conceivably some new ones. We hope to give a full discussion of this situation, particularly as regards automorphisms, in another paper.

UNIVERSITY OF CALIFORNIA, LOS ANGELES.

BIBLIOGRAPHY.

[1] W. Ambrose, "The L_2 system of a unimodular group. I," *Transactions of the American Mathematical Society*, vol. 65 (1949), pp. 27-48.

[2] J. Dixmier, "Algèbres quasi unitaires," *Commentarii Mathematici Helvetici*, vol. 26 (1952), pp. 275-322.

[3] H. A. Dye, "The Radon-Nikodym theorem for finite rings of operators," *Transactions of the American Mathematical Society*, vol. 72 (1952), pp. 243-280.

[4] Samuel Eilenberg and Saunders MacLane, "Cohomology theory in abstract groups. I," *Annals of Mathematics*, vol. 48 (1947), pp. 51-78.

[5] Bent Fuglede and R. V. Kadison, "On a conjecture of Murray and von Neumann," *Proceedings of the National Academy of Sciences*, vol. 37 (1951), pp. 420-425.

[6] Paul R. Halmos and J. von Neumann, "Operator methods in classical mechanics. II," *Annals of Mathematics*, vol. 43 (1942), pp. 322-350.

[7] F. J. Murray and J. von Neumann, "On rings of operators," *Annals of Mathematics*, vol. 37 (1936), pp. 116-229.

[8] J. von Neumann, "On rings of operators. III," *Annals of Mathematics*, vol. 41 (1940), pp. 94-161.

[9] ———, "Zur Algebra der Functionaloperatoren," *Mathematische Annalen*, vol. 102 (1929), pp. 370-427.

[10] I. E. Segal, "A non-commutative extension of abstract integration," *Annals of Mathematics*, vol. 57 (1953), pp. 401-457.

REDUCTION OF ALGEBRAIC VARIETIES WITH RESPECT TO A DISCRETE VALUATION OF THE BASIC FIELD.*

By Goro Shimura.

In the arithmetic theory of algebraic varieties it is useful to have a general theory on "reduction modulo $\mathfrak{p}$" of varieties. Here "reduction" means, roughly spoken, the following process: let V be an algebraic variety defined over a field k with a discrete valuation, and denote by $\mathfrak{p}$ the maximal ideal of that valuation; then we have an algebraic variety $\bar{V}$ over the residue field κ of $\mathfrak{p}$ defined by the equations for V modulo $\mathfrak{p}$; such a variety $\bar{V}$ may be called the variety obtained from the variety V by the reduction modulo $\mathfrak{p}$. When one tries to construct the general theory of reduction in this sense, the first thing to do will be to investigate how the algebraico-geometric properties of V behave in the reduction process. The object of this paper is concerned with that problem.

We shall give a precise definition of the reduction of varieties and the reduction of cycles on a variety. In the case when the ambient varieties V and $\bar{V}$ are both absolutely irreducible, we shall show that the reduction of cycles on V defines a linear mapping from the group of rational V-cycles over k into the group of rational $\bar{V}$-cycles over κ of the same dimension; and shall show that the operations on cycles (the intersection-product, the direct product and the algebraic projection) are all preserved by that mapping (Section 4). If we consider reduction as specialization, this result may be regarded as a specialization-theory of cycles on algebraic varieties, in a certain sense. In fact, from this reduction-theory of cycles we can easily obtain a more general specialization-theory of cycles (Section 5). The latter will be a generalization of the specialization-theory of cycles which has been given by T. Matsusaka [4] and P. Samuel [6]. Our theory may be also called a "local" theory of varieties at a divisor $\mathfrak{p}$, whereas $\mathfrak{p}$ is not a usual divisor on varieties. We shall also show the following fact: let K be a field with a set of infinitely many valuations which satisfies a certain condition (condition (I) in Section 6); if V is an absolutely irreducible variety defined over K, then for almost all those valuations, it remains absolutely irreducible by the reduction process.

* Received February 15, 1954.

M. Deuring has given a reduction-theory of an algebraic function-field of one variable (Deuring [1]) and applied it to his theory of complex multiplication (Deuring [2]). Our results will supply an algebraico-geometric method for these theories.

We proceed in following the method of A. Weil in his book "Foundations of algebraic geometry." [1] We consider specializations over local domains,[2] and by extending Weil's theory to our case, we obtain our results without difficulty. As in Weil's book we shall first deal with affine varieties, and then proceed to abstract and projective varieties.

1. Specialization over an S-domain. We shall call a commutative ring with the identity element an *S-ring* if the set of all non-units forms an ideal. An S-ring which has no zero-divisor will be called an *S-domain.* We shall call a Noetherian S-ring (or S-domain) a *local ring* (or *local domain*). If $\mathfrak{R}$ is a local ring and $\mathfrak{m}$ is the maximal ideal of $\mathfrak{R}$, then we have a topology on $\mathfrak{R}$ by the powers of $\mathfrak{m}$. With respect to this topology, $\mathfrak{R}$ has a *completion* $\mathfrak{R}^*$, which is a local ring containing $\mathfrak{R}$ as subring and subspace, and in which $\mathfrak{R}$ is dense. A valuation ring is an S-domain; and it is a local domain if it is discrete or is a field.

Let $\mathfrak{R}$ be an *S-domain* with the quotient field K and the maximal ideal $\mathfrak{m}$, and $\mathrm{K} = \mathfrak{R}/\mathfrak{m}$ its residue field. For convenience we consider two "*universal domains*" $\boldsymbol{K}$ and $\mathfrak{K}$ which are algebraically closed fields of infinite degree of transcendency over K and K, respectively. We call an element of $\boldsymbol{K}$ (or $\mathfrak{K}$) a *quantity of* $\boldsymbol{K}$ (or $\mathfrak{K}$).[3] Let $(x) = (x_1, \cdots, x_n)$ be a set of n quantities in $\boldsymbol{K}$ and $(\xi) = (\xi_1, \cdots, \xi_n)$ a set of n quantities in $\mathfrak{K}$. We say that (ξ) is a *specialization of* (x) *over* $\mathfrak{R}$ and denote $(x) \xrightarrow{\mathfrak{R}} (\xi)$ if the natural homomorphism of $\mathfrak{R}$ to $\mathfrak{R}/\mathfrak{m}$ can be extended to a homomorphism of $\mathfrak{R}[x]$ onto $\mathrm{K}[\xi]$ which maps (x) on (ξ). It is easy to see that (ξ) is a specialization of (x) over $\mathfrak{R}$ if and only if for every polynomial $F(X)$ in $\mathfrak{R}[X]$ such that $F(x) = 0$ we have $\bar{F}(\xi) = 0$ where $\bar{F}(X)$ is the class of $F(X)$ modulo $\mathfrak{m}$. As in [WF] we add an *infinite* element ∞ both to $\boldsymbol{K}$ and $\mathfrak{K}$ with operations $\infty^{-1} = 0$ and $0^{-1} = \infty$, and by a *generalized quantity* of $\boldsymbol{K}$ (or $\mathfrak{K}$) we understand either a quantity of $\boldsymbol{K}$ (or $\mathfrak{K}$) or ∞. So we say that a set of generalized quantities (x) in $\boldsymbol{K}$ (or (ξ) in $\mathfrak{K}$) is *finite* or *infinite*

[1] Hereafter we shall use the same notations and terminologies as in this book. We shall quote this book as [WF].

[2] Such a specialization has been defined in D. G. Northcott [5] and applied to prove O. Zariski's main theorem on birational correspondences.

[3] The elements of $\boldsymbol{K}$ will be denoted by Latin, those of $\mathfrak{K}$ by Greek letters.

according as none of the x_j (or ξ_j) is ∞ or otherwise. Let (x) be a set of n generalized quantities in $\boldsymbol{K}$ and (ξ) a set of n generalized quantities in $\mathfrak{K}$; we call (ξ) a *specialization of* (x) *over* $\mathfrak{R}$, if there exists a set of n integers $\epsilon_j = \pm 1$, such that $(x') = (x_1^{\epsilon_1}, \cdots, x_n^{\epsilon_n})$ and $(\xi') = (\xi_1^{\epsilon_1}, \cdots, \xi_n^{\epsilon_n})$ are both finite and (ξ') is a specialization of (x') over $\mathfrak{R}$; and also denote by $(x) \xrightarrow{\mathfrak{R}} (\xi)$. We can easily show that if we have $(x) \xrightarrow{K} (x')$ and $(x') \xrightarrow{\mathfrak{R}} (\xi)$ then we have $(x) \xrightarrow{\mathfrak{R}} (\xi)$ and that if we have $(x) \xrightarrow{\mathfrak{R}} (\xi)$ and $(\xi) \xrightarrow{K} (\xi')$ then we have $(x) \xrightarrow{\mathfrak{R}} (\xi')$.

The following theorem is well-known. A proof is given in Weil [7] (Theorem 1.) for a more general case.

THEOREM 1. *Let (x) and (y) be two sets of generalized quantities in $\boldsymbol{K}$. Then every specialization $(x) \xrightarrow{\mathfrak{R}} (\xi)$ can be extended to a specialization $(x, y) \xrightarrow{\mathfrak{R}} (\xi, \eta)$.*

This theorem asserts that, for every S-domain $\mathfrak{R}$ contained in a field K_1, there exists a valuation ring $\mathfrak{R}_1$ with the quotient field K_1 such that $\mathfrak{R}_1 \supset \mathfrak{R}$, $\mathfrak{m}_1 \cap \mathfrak{R} = \mathfrak{m}$ where $\mathfrak{m}$ and $\mathfrak{m}_1$ are respectively the maximal ideals of $\mathfrak{R}$ and $\mathfrak{R}_1$.

We say that (η) is a *specialization of* (y) *over* $(x) \xrightarrow{\mathfrak{R}} (\xi)$ if (ξ, η) is a specialization of (x, y) over $\mathfrak{R}$.

Let (ξ) be a finite specialization of (x) over $\mathfrak{R}$. We call the set $\{F(x)/G(x) \mid \bar{G}(\xi) \neq 0\}$ the *specialization ring of* (ξ) *in* $K(x)$, where $F(X)$ and $G(X)$ are polynomials in $\mathfrak{R}[X]$, and $\bar{G}(X)$ is the class of $G(X)$ modulo $\mathfrak{m}$.[3'] This set is also an S-domain and will be denoted by $[(x) \xrightarrow{\mathfrak{R}} (\xi)]$. If $\mathfrak{R}$ is a local domain, the specialization ring $[(x) \xrightarrow{\mathfrak{R}} (\xi)]$ is also a local domain.

Let (x) be a set of quantities in $\boldsymbol{K}$; we say that (x) is *finite over* $\mathfrak{R}$ if every specialization (ξ) of (x) over $\mathfrak{R}$ is finite. The following proposition is also well-known (Weil [7], Theorem 2.).

PROPOSITION 1. *A set of quantities $(x) = (x_1, \cdots, x_n)$ is finite over $\mathfrak{R}$ if and only if every one of the x_j is integral over $\mathfrak{R}$.*

The following two propositions are easily proved.

PROPOSITION 2. *Let (ξ) be a specialization of (x) over $\mathfrak{R}$. If $\mathfrak{R}$ is a valuation ring, then* $\dim_{\mathrm{K}} (\xi) \leqq \dim_K (x)$.

PROPOSITION 3. *Let (x) be a set of n independent variables over K and (ξ) a set of n independent variables over* K. *If $\mathfrak{R}$ is a (discrete) valuation ring, then $[(x) \xrightarrow{\mathfrak{R}} (\xi)]$ is also a (discrete) valuation ring.*

[3'] Hereafter we use the same notation for the class of a polynomial modulo the maximal ideal. Also we shall use the notation $\bar{k}$ for the algebraic closure of a field k.

LEMMA 1. *Let A be an integral domain and $(t_1, \cdots, t_n)$ a set of n independent variables over A. If A is integrally closed, then the polynomial domain $A[t]$ is also integrally closed.*

Proof. It is sufficient to prove our lemma in the case $n = 1$. It is well-known that an integral domain is integrally closed if and only if it is an intersection of valuation rings. (This follows from Theorem 1 and Proposition 1.) By this fact, we have a representation of A as an intersection $\cap \mathfrak{R}_\omega$ of valuation rings $\mathfrak{R}_\omega$. Denote by K the quotient field of A and by $\mathfrak{R}'_\omega$ the specialization ring $[t \xrightarrow{\mathfrak{R}_\omega} \tau_\omega]$ where τ_ω is an independent variable over the residue field of $\mathfrak{R}_\omega$. Then, by Proposition 3, $\mathfrak{R}'_\omega$ is also a valuation ring for every ω. It can be easily verified that

$$A[t] = \bigcap_\omega \mathfrak{R}_\omega \cap K[t].$$

As is well-known $K[t]$ is integrally closed; so that $A[t]$ is integrally closed.

PROPOSITION 4. *Let $(t_1, \cdots, t_n)$ be a set of n independent variables over K and $(\tau_1, \cdots, \tau_n)$ a set of n quantities in $\mathfrak{K}$. If $\mathfrak{R}$ is an integrally closed S-domain, then the specialization ring $[(t) \xrightarrow{\mathfrak{R}} (\tau)]$ is also integrally closed.*

This follows immediately from Lemma 1.

PROPOSITION 5. *Let (ξ) be a finite specialization of (x) over $\mathfrak{R}$ such that the specialization ring $\mathfrak{S} = [(x) \xrightarrow{\mathfrak{R}} (\xi)]$ is integrally closed. If $\mathfrak{R}$ is a (discrete) valuation ring, and if $\dim_K (x) = \dim_{\mathrm{K}} (\xi)$, then $\mathfrak{S}$ is also a (discrete) valuation ring.*

Proof. Let y be a quantity in $K(x)$ which is not in $\mathfrak{S}$. Then, by Proposition 1 and by our assumption, we have $y \xrightarrow{\mathfrak{S}} \infty$. If η is any finite specialization of y over $\mathfrak{S}$, then, by Proposition 2, we have

$$\dim_{\mathrm{K}} (\xi, \eta) \leqq \dim_K (x, y) = \dim_K (x) = \dim_{\mathrm{K}} (\xi).$$

This shows that η is algebraic over $\mathrm{K}(\xi)$. Let t be an independent variable over $K(x)$ and τ an independent variable over $\mathrm{K}(\xi)$. Put $\mathfrak{T} = [t \xrightarrow{\mathfrak{S}} \tau]$ and $z = (t + y)^{-1}$. By Proposition 4, $\mathfrak{T}$ is integrally closed; and it is easy to see that z is finite over $\mathfrak{T}$; so that z is contained in $\mathfrak{T}$, and has a uniquely determined specialization over $t \xrightarrow{\mathfrak{S}} \tau$. This specialization of z must be 0, since $y \xrightarrow{\mathfrak{S}} \infty$; this shows that y has the only specialization ∞ over $\mathfrak{S}$. Hence y^{-1} is finite over $\mathfrak{S}$, so that y^{-1} is contained in $\mathfrak{S}$, by Proposition 1. Thus we have proved that $\mathfrak{S}$ is a valuation ring. If $\mathfrak{R}$ is discrete, then, by the assumption $\dim_K (x) = \dim_{\mathrm{K}} (\xi)$, $\mathfrak{S}$ is also discrete.

Let K' be any extension of K and let $\mathfrak{R}'$ be an S-domain with the quotient field K' and the maximal ideal $\mathfrak{m}'$, such that $\mathfrak{m}' \cap \mathfrak{R} = \mathfrak{m}$, $\mathfrak{R}' \supset \mathfrak{R}$. When we fix a homomorphism of $\mathfrak{R}'$ into $\mathfrak{K}$ which is an extension of the natural mapping of $\mathfrak{R}$ onto $\mathbf{K}$, we shall say that $\mathfrak{R}'$ is a *prolongation of* $\mathfrak{R}$ *in* K', and call the image of $\mathfrak{R}'$ by that homomorphism the *residue field* of $\mathfrak{R}'$. Thus, when we speak of a prolongation of an S-domain or a valuation ring, it should be remembered that "prolongation" is a combined conception of ring and homomorphism. Also we regard the specialization ring $[(x) \xrightarrow{\mathfrak{R}} (\xi)]$ with its natural mapping $(x) \longrightarrow (\xi)$ as a prolongation of $\mathfrak{R}$.

PROPOSITION 6. *Let $\mathfrak{R}$ be a discrete valuation ring and $\mathfrak{R}'$ a prolongation of $\mathfrak{R}$ in an extension K' of K. If (ξ) is a specialization of (x) over $\mathfrak{R}$, then there exists a generic specialization (x') of (x) over K, such that (ξ) is a specialization of (x') over $\mathfrak{R}'$.*

Proof. We may assume that (x) and (ξ) are both finite. Let $\mathfrak{A}$ be the ideal determined by (x) over the field K. We have a representation of the ideal $K'\mathfrak{A}$ of $K'[X]$ as an intersection of primary ideals $\mathfrak{Q}_i$, belonging respectively to prime ideals $\mathfrak{P}_i$. For every i, we have a set of quantities $(x^{(i)})$ such that $\mathfrak{P}_i$ is the ideal determined by $(x^{(i)})$ over K'. Then we have $(x) \xrightarrow{k} (x^{(i)})$. It is easy to prove that there exists, for every i, a generic specialization $(x'^{(i)})$ of (x) over K such that $(x^{(i)})$ is a specialization of $(x'^{(i)})$ over K'. Hence our proposition is proved if we show that for at least one value of i, $(x^{(i)})$ has (ξ) as a specialization over $\mathfrak{R}'$. Assume that this is impossible. Then there exists, for every i, a polynomial $F_i(X)$ in $\mathfrak{R}'[X]$ such that $F_i(x^{(i)}) = 0$ and that $\bar{F}_i(\xi) \neq 0$. Then $F_i(X) \,\varepsilon\, \mathfrak{P}_i$ for every i; so we can find an integer ρ such that the polynomial $F(X) = \prod_i F_i(X)^\rho$ is contained in $K'\mathfrak{A}$. As $F(X)$ is contained in $\mathfrak{R}'[X]$, we obtain an expression $F(X) = \sum_{\nu=1}^{s} b_\nu G_\nu(X)$ where $b_\nu \,\varepsilon\, \mathfrak{R}'$ and $G_\nu(X) \,\varepsilon\, \mathfrak{R}[X]$. Since $\mathfrak{R}$ is a discrete valuation ring, the finite $\mathfrak{R}$-module $\mathfrak{R}b_1 + \cdots + \mathfrak{R}b_s$ has an $\mathfrak{R}$-basis $(c_1, \cdots, c_r)$ such that $c_1, \cdots, c_r$ are linearly independent over K. Expressing b_ν in a form $b_\nu = \sum_\lambda u_{\nu\lambda} c_\lambda$ with $u_{\nu\lambda} \,\varepsilon\, \mathfrak{R}$, we have $F(X) = \sum_\nu b_\nu G_\nu(X) = \sum_\lambda c_\lambda H_\lambda(X)$, where $H_\lambda(X) = \sum_\nu u_{\nu\lambda} G_\nu(X) \,\varepsilon\, \mathfrak{R}[X]$. Then it follows from $F(X) \,\varepsilon\, K'\mathfrak{A}$ that $H_\lambda(X) \,\varepsilon\, \mathfrak{A}$ for every λ. Then we have $\bar{F}(\xi) = \sum_\lambda \bar{c}_\lambda \bar{H}_\lambda(\xi) = 0$; this is a contradiction.

PROPOSITION 7. *Let $\mathfrak{R}$ be a discrete valuation ring and $\mathfrak{R}'$ a prolongation of $\mathfrak{R}$ in an extension K' of K. Let (x) be a set of quantities such that*

$K(x)$ and K' are linearly disjoint over K, and (ξ) a finite specialization of (x) over $\mathfrak{R}$. Then (ξ) is a specialization of (x) over $\mathfrak{R}'$; and we have $[(x) \xrightarrow{\mathfrak{R}} (\xi)] = K(x) \cap [(x) \xrightarrow{\mathfrak{R}'} (\xi)]$.

Proof. Let $F(X)$ be a polynomial in $\mathfrak{R}'[X]$ such that $F(x) = 0$. We have an expression $F(X) = \sum_{\lambda=1}^{r} c_\lambda H_\lambda(X)$ where $c_\lambda \in \mathfrak{R}'$, $H_\lambda(X) \in \mathfrak{R}[X]$ for every λ. By the same procedure as in the proof of Proposition 6, we may assume that $c_1, \cdots, c_r$ are linearly independent over K. Then, by our assumption that K' and $K(x)$ are linearly disjoint over K, the relation $\sum_\lambda c_\lambda H_\lambda(x) = F(x) = 0$ implies that $H_\lambda(x) = 0$ for every λ. Since (ξ) is a specialization of (x) over $\mathfrak{R}$, we have $\bar{F}(\xi) = \sum_\lambda \bar{c}_\lambda \bar{H}_\lambda(\xi) = 0$; this proves the first assertion. Now let y be a quantity in $K(x) \cap [(x) \xrightarrow{\mathfrak{R}'} (\xi)]$; then we have an expression $y = P(x)/Q(x)$ with $P(X)$ and $Q(X)$ in $\mathfrak{R}'[X]$ and $\bar{Q}(\xi) \neq 0$. Let $(b_1, \cdots, b_s)$ be the set of all coefficients of P and Q; as in the proof of Proposition 6, we have an $\mathfrak{R}$-basis $d_1, \cdots, d_t$ of $\mathfrak{R}b_1 + \cdots + \mathfrak{R}b_s$ which are linearly independent over K. Then we have expressions $P(X) = \sum_\nu d_\nu F_\nu(X)$, $Q(X) = \sum_\nu d_\nu G_\nu(X)$ where the $F_\nu(X)$ and the $G_\nu(X)$ are in $\mathfrak{R}[X]$. By our assumption, from the relation $\sum_\nu d_\nu(F_\nu(x) - yG_\nu(x)) = 0$ follows that $F_\nu(x) = yG_\nu(x)$ for every ν. Since $\bar{Q}(\xi) \neq 0$, we have $\bar{G}_\nu(\xi) \neq 0$ for some ν; for that ν we have $y = F_\nu(x)/G_\nu(x)$; this proves the second assertion.

PROPOSITION 8. *Let $K(x)$ and $K(y)$ be two extensions of K which are linearly disjoint over K. If $\mathfrak{R}$ is a discrete valuation ring, then (ξ, η) is a specialization of (x, y) over $\mathfrak{R}$ if and only if (ξ) is a specialization of (x) over $\mathfrak{R}$ and (η) is a specialization of (y) over $\mathfrak{R}$.*

Proof. We shall prove only the direct part since the converse is obvious. We may assume that (ξ) and (η) are both finite. Put $K' = K(y)$ and $\mathfrak{R}' = [(y) \xrightarrow{\mathfrak{R}} (\eta)]$. We may consider $\mathfrak{R}'$ is a prolongation of $\mathfrak{R}$ in K'. Then our proposition is an immediate consequence of Proposition 7.

PROPOSITION 9. *Let $\mathfrak{R}$ be a discrete valuation ring. For any finitely generated extension K' of K, there exist a finitely generated extension K' of K and a prolongation $\mathfrak{R}'$ of $\mathfrak{R}$ in K' which is a discrete valuation ring, such that K' is the residue field of $\mathfrak{R}'$.*

Proof. Our proposition follows from Proposition 3 if K' is purely transcendental over K; so that we have only to prove our proposition in case

where K' is a simple algebraic extension $\mathrm{K}(\xi)$ of K. Let $\bar{F}(X)=0$ be an irreducible equation for ξ over K; where we may assume that $\bar{F}$ is the class of a polynomial F in $\mathfrak{R}[X]$ of the same degree as $\bar{F}$, modulo $\mathfrak{m}$. Let x be a root of the equation $F(X)=0$ in $\bar{K}$, and put $K'=K(x)$. We have a discrete valuation ring $\mathfrak{R}'$ in K' with the maximal ideal $\mathfrak{m}'$, such that $\mathfrak{R}'\supset\mathfrak{R}$, $\mathfrak{m}'\cap\mathfrak{R}=\mathfrak{m}$. Since the class of x modulo $\mathfrak{m}'$ satisfies the equation $\bar{F}(X)=0$, we have $[\mathrm{K}':\mathrm{K}]\leqq[\mathfrak{R}'/\mathfrak{m}':\mathfrak{R}/\mathfrak{m}]$. It is well-known that $[\mathfrak{R}'/\mathfrak{m}':\mathfrak{R}/\mathfrak{m}]\leqq[K':K]$; so, by our definition of K', we have $[\mathrm{K}':\mathrm{K}]=[\mathfrak{R}'/\mathfrak{m}':\mathfrak{R}/\mathfrak{m}]=[K':K]$. This shows that $\mathfrak{R}'/\mathfrak{m}'$ is isomorphic to K' over K; so our proposition is proved.

2. Multiplicity of a proper specialization. As before, let $\mathfrak{R}$ be an S-domain with the quotient field K and the residue field K. We say that (η) is an *isolated specialization of* (y) *over* $\mathfrak{R}$, if whenever we have $(y)\xrightarrow{\mathfrak{R}}(\eta')$ and $(\eta')\xrightarrow{\mathrm{K}}(\eta)$, we also have $(\eta)\xrightarrow{\mathrm{K}}(\eta')$. A finite specialization of (y) over $\mathfrak{R}$ is called a *proper specialization of* (y) *over* $\mathfrak{R}$ if it is isolated and algebraic over K.

Let (y) be a set of algebraic quantities over K and let $(y^{(1)},\cdots,y^{(n)})$ be a complete set of conjugates of (y) over K. Let (η) be a specialization of (y) over $\mathfrak{R}$. If there exists a number μ, such that for every specialization $(\eta^{(1)},\cdots,\eta^{(n)})$ of $(y^{(1)},\cdots,y^{(n)})$ over $\mathfrak{R}$, the set (η) occurs exactly μ times among $(\eta^{(\nu)})$, then we call the number μ the *multiplicity of* (η) *as a specialization of* (y) *over* $\mathfrak{R}$. The main object of this section is to show that a proper specialization over a certain local domain has a well-defined multiplicity.

PROPOSITION 10. *Let $\mathfrak{R}$ be an integrally closed S-domain with the quotient field K, and (y) a set of algebraic quantities over K. If (y) is finite over $\mathfrak{R}$, then every specialization of (y) over $\mathfrak{R}$ is proper and has a multiplicity defined above.*

Proof. By Proposition 1 of Section 1, (y) is integral over $\mathfrak{R}$; so that every specialization of (y) over $\mathfrak{R}$ is finite algebraic over K. From this follows that every specialization of (y) over $\mathfrak{R}$ is proper. As for the assertion concerned with the multiplicity, first we shall prove it in case where the set (y) consists of a single quantity y. Let $F(Y)=0$ be the irreducible equation for y over K with the leading coefficient 1. Then $F(Y)$ is a polynomial contained in $\mathfrak{R}[Y]$ since $\mathfrak{R}$ is integrally closed. It can be easily verified that every specialization of the complete set of conjugates of y coincides with the set of all roots of the equation $\bar{F}(Y)=0$. This proves our proposition in the case when (y) consists of one quantity. To prove the general case we

put $z = \sum_i t_i y_i$ where (t) is a set of independent variables over K. Let (τ) be a set of independent variables over K, and denote by $\mathfrak{S}$ the specialization ring $[(t) \xrightarrow{\mathfrak{R}} (\tau)]$. Then, by Proposition 4, $\mathfrak{S}$ is also an integrally closed S-domain; and it is easy to see that z is finite over $\mathfrak{S}$. If we denote by $(y^{(1)}, \cdots, y^{(n)})$ the complete set of conjugates of (y) over K and put $z_\nu = \sum_i t_i y_i^{(\nu)}$, then the set $(z_1, \cdots, z_n)$ consists of a repetition in a certain number of times of the complete set of conjugates of z over $K(t)$. So the general case is reduced to the case of one quantity.

Let $\mathfrak{R}$ be a local domain such that the completion $\mathfrak{R}^*$ of $\mathfrak{R}$ has no zero-divisor. We identify the quotient field K of $\mathfrak{R}$ with a subfield of the quotient field Ω of $\mathfrak{R}^*$ in the usual manner. The following two propositions are generalizations of Theorem 1 and Theorem 3 of [WF] Chapter III, Section 3. Proofs by the same method as in [WF] have been stated in Northcott [5] in a general form.

Proposition 11. *Let $\mathfrak{R}^*$ be a complete local domain with the quotient field Ω and (y) a set of elements in some field containing Ω. If (y) has a proper specialization over $\mathfrak{R}^*$, then (y) is integral over $\mathfrak{R}^*$; and any two specializations of (y) over $\mathfrak{R}^*$ are conjugates of each other over the residue field of $\mathfrak{R}^*$.*

Proposition 12. *Let $\mathfrak{R}$ be a local domain such that the completion $\mathfrak{R}^*$ of $\mathfrak{R}$ has no zero-divisor, (y) a set of generalized quantities which is algebraic over K, and (η) a specialization of (y) over $\mathfrak{R}$. Let Ω be the quotient field of $\mathfrak{R}^*$ and $\bar{\Omega}$ the algebraic closure of Ω. Then there exists an isomorphism of $K(y)$ over K into $\bar{\Omega}$ such that if (y') is the image of (y) we have $(y') \xrightarrow{\mathfrak{R}^*} (\eta)$.*

Now we consider specializations over a special type of local domains. Let $\mathfrak{o}$ be a discrete valuation ring with the quotient field k and the maximal ideal $\mathfrak{p}$, and let $\kappa = \mathfrak{o}/\mathfrak{p}$ be its residue field. Let $(x_1, \cdots, x_n)$ be a set of independent variables over k, and denote by $\mathfrak{R}$ the specialization ring $[(x_1, \cdots, x_n) \xrightarrow{\mathfrak{o}} (0, \cdots, 0)]$ and by $\mathfrak{R}^*$ its completion. Then $\mathfrak{R}^*$ is the ring of the formal power-series $\sum a_{(i)}^* x_1^{i_1} \cdots x_n^{i_n}$ with $a_{(i)}^*$ in the completion $\mathfrak{o}^*$ of $\mathfrak{o}$. The complete local domain $\mathfrak{R}^*$ is a regular local ring in Krull's sense [4] and is integrally closed.

Proposition 13. *Let $\mathfrak{R}^*$ be the completion of the specialization ring $[(x_1, \cdots, x_n) \xrightarrow{\mathfrak{o}} (0, \cdots, 0)]$ in the above notations; let Ω be the quotient*

[4] Krull [3].

field of $\mathfrak{R}^*$ *and* (y) *a set of algebraic elements over* Ω. *If* (η) *is a proper specialization of* (y) *over* $\mathfrak{R}^*$, *then* (η) *has a multiplicity which is a multiple of* $[\kappa(\eta):\kappa]_i$.

Proof. By Proposition 11, (y) is integral over $\mathfrak{R}^*$; hence, by Proposition 10, every specialization (η') of (y) over $\mathfrak{R}^*$ has a multiplicity. Let $(y^{(1)},\cdots,y^{(d)})$ be a complete set of conjugates of (y) over Ω and $(\eta^{(1)},\cdots,\eta^{(d)})$ a specialization of $(y^{(1)},\cdots,y^{(d)})$ over $\mathfrak{R}^*$. By Proposition 11, the set $(\eta^{(1)},\cdots,\eta^{(d)})$ consists of conjugates of (η) over κ. Everyone of conjugates of (η) over κ is a specialization of (y) over $\mathfrak{R}^*$; so that it has a positive multiplicity as a specialization of (y) over $\mathfrak{R}^*$. Thus $(\eta^{(1)},\cdots,\eta^{(d)})$ contains all the conjugates of (η) over κ; and it is easy to see that all the conjugates of (η) occur in $(\eta^{(\nu)})$ in the same multiplicity. Hence our proposition is proved when we show that $d=[\Omega(y):\Omega]$ is a multiple of $[\kappa(\eta):\kappa]$. Let (t) be a set of n independent variables over k and (τ) a set of n independent variables over κ. We denote by $\mathfrak{R}_1$ the specialization ring $[(t)\xrightarrow{\mathfrak{o}}(\tau)]$ and by $\mathfrak{R}_1^*$ its completion. By Proposition 3 of Section 1, $\mathfrak{R}_1$ is a discrete valuation ring. We may regard the completion $\mathfrak{o}^*$ of $\mathfrak{o}$ as a subring of $\mathfrak{R}_1^*$. Now we shall define an isomorphic mapping f of $\mathfrak{R}^*$ over $\mathfrak{o}^*$ into $\mathfrak{R}_1^*$. For an element

$$A=\sum a_{(i)}{}^*x_1{}^{i_1}\cdots x_n{}^{i_n}\,\varepsilon\,\mathfrak{R}^*,$$

we define

$$f(A)=\sum a_{(i)}{}^*\pi^{i_1+\cdots+i_n}t_1{}^{i_1}\cdots t_n{}^{i_n}$$

where π is a prime element in $\mathfrak{o}$. It is easy to see that this mapping f is actually an isomorphic mapping into $\mathfrak{R}_1^*$. Then f is extended to an isomorphism of Ω into the quotient field Ω_1 of $\mathfrak{R}_1^*$, and is also extended to an isomorphism g of $\bar{\Omega}$ into $\bar{\Omega}_1$. We denote by (y') the image of (y) by g and by $(y'^{(1)},\cdots,y'^{(d)})$ the image of $(y^{(1)},\cdots,y^{(d)})$. If (ζ) is a specialization of $(y'^{(\nu)})$ over $\mathfrak{R}_1^*$, then (ζ) is a specialization of (y) over $\mathfrak{R}^*$; hence, by Proposition 11, (ζ) is a conjugate of (η) over κ. Now it is well-known that $[\Omega_1(y'^{(\nu)}):\Omega_1]$ is a multiple of $[\kappa(\tau,\zeta):\kappa(\tau)]$ since $\mathfrak{R}_1^*$ is a complete discrete valuation ring; the latter number is clearly equal to $[\kappa(\eta):\kappa]$, while $[\Omega(y):\Omega]$ is a sum of several $[\Omega_1(y'^{(\nu)}):\Omega_1]$; this completes our proof.

The following theorem is an extension of Theorem 4 of [WF] Chapter III, Section 4, and is basic for our whole theory.

THEOREM 2. *Let* (x) *be a set of* n *independent variables over* k *and* (y) *a set of algebraic quantities over* $k(x)$. *Let* (ξ) *be a finite specialization of* (x) *over* $\mathfrak{o}$ *and denote by* $\mathfrak{R}$ *the specialization ring* $[(x)\xrightarrow{\mathfrak{o}}(\xi)]$. *If* (η)

is a proper specialization of (y) *over* $\mathfrak{R}$, *then it has a multiplicity which is a multiple of* $[\kappa(\xi,\eta):\kappa(\xi)]_i$.[5]

Proof. We first assume that (ξ) is contained in κ. Then we have a set of quantities (a) in $\mathfrak{o}$ such that $(a) \xrightarrow{\mathfrak{o}} (\xi)$. Replacing the set (x_j) by $(x_j - a_j)$, we may assume that $(\xi) = (0)$. In that special case, we can obtain our theorem by Proposition 12 and Proposition 13, in the same procedure as in the proof of Proposition 7 of [WF] Chapter III, Section 3. Now we shall prove the general case. Let s be the dimension of (ξ) over κ; if s is not 0, we may assume that $\xi_1, \cdots, \xi_s$ are independent variables over κ, and that (ξ) is algebraic over $\kappa(\xi_1, \cdots, \xi_s)$. By Proposition 3 of Section 1, the specialization ring $[(x_1, \cdots, x_s) \xrightarrow{\mathfrak{o}} (\xi_1, \cdots, \xi_s)]$ is a discrete valuation ring; if we denote it by $\mathfrak{o}_1$, we have $\mathfrak{R} = [(x_{s+1}, \cdots, x_n) \xrightarrow{\mathfrak{o}_1} (\xi_{s+1}, \cdots, \xi_n)]$. Hence, it is sufficient to prove our theorem in case where (ξ) is algebraic over κ. Suppose that (ξ) is algebraic over κ. By Proposition 9 of Section 1, we can find an algebraic extension k' of k and a valuation ring $\mathfrak{o}'$ which is a prolongation of $\mathfrak{o}$ in k', such that the residue field κ' of $\mathfrak{o}'$ is $\kappa(\xi)$. Let $(y^{(1)}, \cdots, y^{(d)})$ be the complete set of conjugates of (y) over $k(x)$ and $(\eta^{(1)}, \cdots, \eta^{(d)})$ a specialization of $(y^{(1)}, \cdots, y^{(d)})$ over $\mathfrak{R}$. Then by Proposition 6 of Section 1, there exists a generic specialization $(x', y'^{(1)}, \cdots, y'^{(d)})$ of $(x, y^{(1)}, \cdots, y^{(d)})$ such that $(x', y'^{(1)}, \cdots, y'^{(d)}) \xrightarrow{\mathfrak{o}'} (\xi, \eta^{(1)}, \cdots, \eta^{(d)})$. Since k' is algebraic over k, (x) is a generic specialization of (x') over k', and is extended to a generic specialization $(x, y''^{(1)}, \cdots, y''^{(d)})$ of $(x', y'^{(1)}, \cdots, y'^{(d)})$ over k'. Then $(x, y''^{(1)}, \cdots, y''^{(d)})$ is a generic specialization of $(x, y^{(1)}, \cdots, y^{(d)})$ over k and has the specialization $(\xi, \eta^{(1)}, \cdots, \eta^{(d)})$ over $\mathfrak{o}'$. The set $(y''^{(1)}, \cdots, y''^{(d)})$ is a permutation of $(y^{(1)}, \cdots, y^{(d)})$ since $(y^{(1)}, \cdots, y^{(d)})$ is the complete set of conjugates of (y) over $k(x)$. Therefore, it is sufficient to prove that for every specialization $(\eta^{(1)}, \cdots, \eta^{(d)})$ of $(y^{(1)}, \cdots, y^{(d)})$ over $(x) \xrightarrow{\mathfrak{o}'} (\xi)$ the set (η) occurs in $(\eta^{(1)}, \cdots, \eta^{(d)})$ in the same times μ, and that μ is a multiple of $[\kappa(\xi,\eta):\kappa(\xi)]_i$. Now the set $(y^{(1)}, \cdots, y^{(d)})$ consists of several complete sets of conjugates of sets $(y^{(\nu)})$ over $k'(x)$. Since $\kappa' = \kappa(\xi)$, we have $[\kappa(\xi,\eta):\kappa(\xi)]_i = [\kappa'(\eta):\kappa']_i$. Thus what we have to prove is reduced to the case in which our theorem is already proved.

The following three theorems are generalizations of Proposition 10, Proposition 11 and Theorem 5 in [WF] Chapter III, Section 4, and can be proved by the same arguments as there.

---

[5] This theorem holds for any regular local ring $\mathfrak{R}$. It can be easily verified that the specialization ring $[(x) \xrightarrow{\mathfrak{o}} (\xi)]$ in our theorem is a regular local ring.

THEOREM 3. *Let (x) be a set of independent variables over k, (y) and (z) two sets of algebraic quantities over $k(x)$, and (ξ, η) a finite specialization of (x, y) over $\mathfrak{o}$. Assume that (η) is a proper specialization, of multiplicity μ, of (y) over $(x) \xrightarrow{\mathfrak{o}} (\xi)$, and that (z) is finite over $(x, y) \xrightarrow{\mathfrak{o}} (\xi, \eta)$. Then the specializations $(\zeta^{(\sigma)})$ of (z) over $(x, y) \xrightarrow{\mathfrak{o}} (\xi, \eta)$ are in a finite number; for every σ, $(\eta, \zeta^{(\sigma)})$ is a proper specialization of (y, z) over $(x) \xrightarrow{\mathfrak{o}} (\xi)$; and if μ_σ is the multiplicity of that specialization, we have the relation*

$$\sum_\sigma \mu_\sigma = \mu[k(x, y, z) : k(x, y)].$$

THEOREM 4. *Let (x) and (z) be two sets of independent variables over k; let (y) be a set of algebraic quantities over $k(x)$ and (w) a set of algebraic quantities over $k(z)$. Assume that $k(x, y)$ and $k(z, w)$ are linearly disjoint over k. Let (ξ, ζ) be a finite specialization of (x, z) over $\mathfrak{o}$; let (η) be a proper specialization of (y), of multiplicity μ, over $(x) \xrightarrow{\mathfrak{o}} (\xi)$, and let (ω) be a proper specialization of (w), of multiplicity ν, over $(z) \xrightarrow{\mathfrak{o}} (\zeta)$. Then (η, ω) is a proper specialization of (y, w) over $(x, z) \xrightarrow{\mathfrak{o}} (\xi, \zeta)$; and the multiplicity of this specialization is equal to $\mu\nu$.*

THEOREM 5. *Let (x) be a set of independent variables over k and (y) a set of m algebraic quantities over $k(x)$. Let (ξ, η) be a finite specialization of (x, y) over $\mathfrak{o}$, and assume that there are m polynomials $F_j(X, Y)$ in $\mathfrak{o}[X, Y]$, such that $F_j(x, y) = 0$ for $1 \leqq j \leqq m$ and that the determinant $|\partial F_j/\partial Y_h(\xi, \eta)|$ is not 0. Then (η) is a proper specialization of (y) over $(x) \xrightarrow{\mathfrak{o}} (\xi)$; and its multiplicity is 1.*

PROPOSITION 14. *Let (x) be a set of independent variables over k and (y) a set of algebraic quantities over $k(x)$. Let (ξ) be a finite specialization of (x) over $\mathfrak{o}$ and (η) a proper specialization of (y) over $(x) \xrightarrow{\mathfrak{o}} (\xi)$. Then the following two conclusions hold.*

(I) *Let (x') be a finite specialization of (x) over k such that (ξ) is a specialization of (x') over $\mathfrak{o}$. Then there exists a specialization (x', y') of (x, y) over k, which has (ξ, η) as a specialization over $\mathfrak{o}$.*

(II) *Let (ξ') be a finite specialization of (x) over $\mathfrak{o}$ such that (ξ) is a specialization of (ξ') over κ. Then there exists a specialization (ξ', η') of (x, y) over $\mathfrak{o}$, which has (ξ, η) as a specialization over κ.*

This is also proved as in Proposition 12 of [WF] Chapter III, Section 4.

PROPOSITION 15. *Let (x) be a set of n quantities of dimension r over k. Let the t_{ij} $(1 \leqq i \leqq r, 1 \leqq j \leqq n)$ be rn independent variables over $k(x)$*

and the τ_{ij} $(1 \leqq i \leqq r, 1 \leqq j \leqq n)$ *rn independent variables over* κ. *Put* $\mathfrak{o}' = [(t) \xrightarrow{\mathfrak{o}} (\tau)]$, *and* $y_i = \sum_j t_{ij} x_j$ *for* $1 \leqq i \leqq r$. *If* (ξ, η) *is a finite specialization of* (x, y) *over* $\mathfrak{o}'$, *then* (ξ) *is a proper specialization of* (x) *over* $(y) \xrightarrow{\mathfrak{o}'} (\eta)$.

Proof. It is enough to prove that if (ξ, η) is a finite specialization of (x, y) over $\mathfrak{o}'$ then (ξ) is algebraic over $\kappa(\tau, \eta)$. Let (ξ, η) be a finite specialization of (x, y) over $\mathfrak{o}'$ and s the dimension of (ξ) over κ. Then by Proposition 2 of Section 1, we have $s \leqq r$. Let (ξ') be a generic specialization of (ξ) over κ such that (ξ') and (τ) are independent over κ. Put $\eta_i' = \sum_j \tau_{ij} \xi_j'$ for $1 \leqq i \leqq r$. Since $(\xi', \tau) \xrightarrow{\kappa} (\xi, \tau)$, we have $(\xi', \tau, \eta') \xrightarrow{\kappa} (\xi, \tau, \eta)$. Now by Proposition 24 of [WF] Chapter II, Section 5, (ξ') is finite over every finite specialization of $(\eta_1', \cdots, \eta_s')$ with reference to $\kappa(\tau_{11}, \cdots, \tau_{sn})$. Hence (ξ) is algebraic over $\kappa(\tau, \eta)$.

PROPOSITION 16. *Let* (x), (y), (t), (τ) *and* $\mathfrak{o}'$ *be the same as in Proposition* 15. *Let the* s_j $(1 \leqq j \leqq n)$ *be* n *independent variables over* $k(t, x)$ *and the* σ_j $(1 \leqq j \leqq n)$ n *independent variables over* $\kappa(\tau)$. *Put* $\mathfrak{o}'' = [(s) \xrightarrow{\mathfrak{o}'} (\sigma)]$ *and* $z = \sum_j s_j x_j$. *Let* (η, ζ) *be a finite specialization of* (y, z) *over* $\mathfrak{o}''$. *Then* ζ *is a proper specialization of* z *over* $(y) \xrightarrow{\mathfrak{o}''} (\eta)$; *and* (x) *is finite over* $(y, z) \xrightarrow{\mathfrak{o}''} (\eta, \zeta)$. *Let* (ξ) *be a specialization of* (x) *over* $(y, z) \xrightarrow{\mathfrak{o}''} (\eta, \zeta)$ *such that* (ξ) *and* (τ, σ) *are independent over* κ. *If* $k(x)$ *is separably generated over* k, *then we have* $k(t, s, x) = k(t, s, y, z)$; *and the multiplicity of* (ξ) *as a specialization of* (x) *over* $(y) \xrightarrow{\mathfrak{o}'} (\eta)$ *is equal to the multiplicity of* ζ *as a specialization of* z *over* $(y) \xrightarrow{\mathfrak{o}''} (\eta)$.

Proof. By the same method as in the proof of Proposition 24 of [WF] Chapter II, Section 5, we can prove that (x) is finite over $(y, z) \xrightarrow{\mathfrak{o}''} (\eta, \zeta)$. Let ξ be a specialization of (x) over $(y, z) \xrightarrow{\mathfrak{o}''} (\eta, \zeta)$. Then, by Proposition 15, (ξ) is algebraic over $\kappa(\tau, \eta)$; so that $\zeta = \sum_j \sigma_j \xi_j$ is algebraic over $\kappa(\tau, \sigma, \eta)$. This shows that every finite specialization of z over $(y) \xrightarrow{\mathfrak{o}''} (\eta)$ is algebraic over $\kappa(\tau, \sigma, \eta)$. Hence ζ is a proper specialization of z over $(y) \xrightarrow{\mathfrak{o}''} (\eta)$. Suppose that $k(x)$ is separably generated over k. Then $k(t, x)$ is separably algebraic over $k(t, y)$. Denote by $(x^{(1)}, \cdots, x^{(d)})$ the complete set of conjugates of (x) over $k(t, y)$, and put $z^{(\nu)} = \sum_j s_j x_j^{(\nu)}$ for $1 \leqq \nu \leqq d$; then it is easy to see that $(z^{(1)}, \cdots, z^{(d)})$ is the complete set of conjugates of z over $k(t, s, y)$. This shows $[k(t, s, y, z) : k(t, s, y)] = d = [k(t, s, x) : k(t, s, y)]$; so we have $k(t, s, x) = k(t, s, y, z)$. Let (ξ) be a specialization of (x)

over $(y,z)\xrightarrow{\mathfrak{o}''}(\eta,\zeta)$ such that (ξ) and (τ,σ) are independent over κ. Let $(\xi^{(1)},\cdots,\xi^{(d)})$ be a specialization of $(x^{(1)},\cdots,x^{(d)})$ over $(y)\xrightarrow{\mathfrak{o}'}(\eta)$. We extend this specialization to a specialization

$$(x^{(1)},\cdots,x^{(d)},y,z^{(1)},\cdots,z^{(d)})\xrightarrow{\mathfrak{o}''}(\xi^{(1)},\cdots,\xi^{(d)},\eta,\zeta^{(1)},\cdots,\zeta^{(d)}).$$

If $(\xi^{(\nu)})=(\xi)$, then we have $\zeta^{(\nu)}=\sum_j\sigma_j\xi_j^{(\nu)}=\sum_j\sigma_j\xi_j=\zeta$. Conversely, if $\zeta^{(\nu)}=\zeta$, then we have $(x,y,z,t,s)\xrightarrow{k}(x^{(\nu)},y,z^{(\nu)},t,s)\xrightarrow{\mathfrak{o}}(\xi^{(\nu)},\eta,\zeta,\tau,\sigma)$. Since (x) is finite over $(y,z)\xrightarrow{\mathfrak{o}''}(\eta,\zeta)$, $(\xi^{(\nu)})$ is finite; so we have $\zeta=\sum_j\sigma_j\xi_j^{(\nu)}$. By Proposition 15, $(\xi^{(\nu)})$ is algebraic over $\kappa(\tau,\eta)$; since $\eta_i=\sum_j\tau_{ij}\xi_j$, $(\xi^{(\nu)})$ is also algebraic over $\kappa(\tau,\xi)$. By our assumption, (σ) is a set of independent variables over $\kappa(\tau,\xi)$; so that from $\sum_j\sigma_j\xi_j^{(\nu)}=\sum_j\sigma_j\xi_j$ follows $\xi_j^{(\nu)}=\xi_j$ $(1\leqq j\leqq n)$. Thus we have proved that $\zeta^{(\nu)}=\zeta$ if and only if $(\xi^{(\nu)})=(\xi)$. This proves the final assertion of our proposition.

By Proposition 14 and by Proposition 15, the following theorem can be proved in the same procedure as in the proof of Proposition 13 in [WF] Chapter III, Section 4.

THEOREM 6. *Let (x) and (y) be two sets of quantities, and (ξ,η) a finite specialization of (x,y) over $\mathfrak{o}$. Then if (η) is an isolated specialization of (y) over $(x)\xrightarrow{\mathfrak{o}}(\xi)$, the dimension of (η) over $\kappa(\xi)$ is at least equal to that of (y) over $k(x)$.*

PROPOSITION 17. *Let (y) be a set of independent variables over k and z an algebraic quantity over $k(y)$. Let $F(Y,Z)=0$ be an irreducible equation for (y,z) over k and assume that F is a primitive polynomial in $\mathfrak{o}[Y,Z]$. Let ζ be a proper specialization of z, of multiplicity 1, over a finite specialization $(y)\xrightarrow{\mathfrak{o}}(\eta)$. Then we have $\partial\bar{F}/\partial Z(\eta,\zeta)\neq 0$; and $[(y,z)\xrightarrow{\mathfrak{o}}(\eta,\zeta)]$ is integrally closed.*

This proposition is a translation of Proposition 19 in [WF] Chapter V, Section 3 to our case and can be proved by the same argument as there.

3. Reduction of affine varieties. Let k be a field with a discrete valuation, and $\mathfrak{o}$ be its valuation ring. We denote by $\mathfrak{p}$ the maximal ideal of $\mathfrak{o}$ and by κ the residue field $\mathfrak{o}/\mathfrak{p}$. We fix this field k and the valuation ring $\mathfrak{o}$; in the following we shall use these notations k, $\mathfrak{o}$, $\mathfrak{p}$ and κ always in this sense; and whenever we speak of a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ we presuppose that $\mathfrak{o}'$ is also a discrete valuation ring.

Let S^n and $\mathfrak{S}^n$ be the affine n-spaces defined with respect to the field k and κ, respectively. First we define the reduction of a variety as a point set.

Let U be a bunch[6] in S^n which is normally algebraic over k. We call a bunch attached to a set $\{(\alpha) \mid (\alpha) \varepsilon \mathfrak{S}^n, (a) \xrightarrow{\mathfrak{o}} (\alpha)$ for some $(a) \varepsilon U\}$ the *bunch obtained from U by the reduction with respect to* $\mathfrak{p}$ (or $\mathfrak{o}$), or the *reduced bunch,* and denote it by $\bar{U}$. It may happen that $\bar{U}$ is an empty set even if U is not empty.

THEOREM 7. *Let U be a bunch in S^n which is normally algebraic over k, and let $\mathfrak{a}$ be the ideal $\{F(X) \mid F(X) \varepsilon \mathfrak{o}[X], F(a) = 0$ for every $(a) \varepsilon U\}$ in $\mathfrak{o}[X]$. Then, we have $\bar{U} = \{(\alpha) \mid (\alpha) \varepsilon \mathfrak{S}^n, \bar{F}(\alpha) = 0$ for every $F(X) \varepsilon \mathfrak{a}\}$; so that $\bar{U}$ is a bunch in $\mathfrak{S}^n$ which is normally algebraic over κ. Furthermore if k' is any extension of k and $\mathfrak{o}'$ is a prolongation of $\mathfrak{o}$ in k', then we have $\bar{U} = \{(\alpha) \mid (\alpha) \varepsilon \mathfrak{S}^n, (a) \xrightarrow{\mathfrak{o}'} (\alpha)$ for some $(a) \varepsilon U\}$.*

Proof. By our definition of $\bar{U}$, it is obvious that if $(\alpha) \varepsilon \bar{U}$ then $\bar{F}(\alpha) = 0$ for every $F(X) \varepsilon \mathfrak{a}$. Now we express U as the union of prime rational cycles U_i over k: $U = U_1 \cup \cdots \cup U_h$. Let $(x^{(i)})$ be a generic point of U_i over k for every i; then we have $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_h$ where

$$\mathfrak{a}_i = \{F(X) \mid F(X) \varepsilon \mathfrak{o}[X], F(x^{(i)}) = 0\}$$

for every i. Suppose that, for every i, (α) is not a specialization of $(x^{(i)})$ over $\mathfrak{o}$. Then there exists, for every i, a polynomial $F_i(X)$ in $\mathfrak{a}_i$ such that $\bar{F}_i(\alpha) \neq 0$. If we put $F(X) = \prod_i F_i(X)$ we have $F(X) \varepsilon \mathfrak{a}$ and $\bar{F}(\alpha) \neq 0$. This proves our first assertion. The second assertion follows from our definition of $\bar{U}$ and Proposition 6 of Section 1.

By this theorem the reduced bunch $\bar{U}$ is invariant under the extension of the basic field k and the prolongation of $\mathfrak{o}$ in that extension. This property of reduction also holds for reduction of cycles which is to be defined later.

PROPOSITION 18. *Let U and V be bunches which are normally algebraic over k. Then we have*

i) *If U and V are in the same ambient space S^n, then we have $\overline{U \cup V} = \bar{U} \cup \bar{V}$, $\overline{U \cap V} \subset \bar{U} \cap \bar{V}$.*

ii) *If U is in S^n and V is in S^m, then we have $\overline{U \times V} = \bar{U} \times \bar{V}$.*

Proof. The assertion i) is an immediate consequence of our definition. Now we shall prove ii). Let k' be a finite algebraic extension of k such that

[6] From now on we shall identify a bunch with the point set attached to that bunch. Also we shall use the term "prime rational cycle" for the bunch whose components are components of that cycle.

all the components of U and V are defined over k'. We have representations $U=\bigcup_i U_i$ and $V=\bigcup_j V_j$ where U_i and V_j are varieties defined over k'. Let $\mathfrak{o}'$ be a prolongation of $\mathfrak{o}$ in k', we consider the reduction with respect to $\mathfrak{o}'$. Since $\overline{U\times V}=\bigcup_{i,j}\overline{U_i\times V_j}$, it is sufficient to prove that $\overline{U_i\times V_j}=\overline{U}_i\times\overline{V}_j$ for every i and j. This is proved by Proposition 8 of Section 1 and by our definition.

PROPOSITION 19. *Let U be a bunch in S^n which is normally algebraic over k and assume that the components of U are all of dimension r. If $\bar{U}$ is not empty, then the components of $\bar{U}$ are all of dimension r.*

This is an immediate consequence of Theorem 6 of Section 2.

Let A be a prime rational S^n-cycle over k. Now we shall define a rational $\mathfrak{S}^n$-cycle $\rho(A)$ over κ which will be called the cycle obtained from A by the reduction with respect to $\mathfrak{p}$ (or $\mathfrak{o}$).

LEMMA 2. *Let A^r be a prime rational S^n-cycle over a field K. Let the $F_i(X)=\sum_j c_{ij}X_j$ $(1\leqq i\leqq r)$ be r linearly independent linear forms in $K[X]$, and (v) a set of r independent variables over K; and let L^{n-r} be the variety defined by the set of equations $F_i(X)-v_i=0$ $(1\leqq i\leqq r)$. Then, if there is a point P in $A\cap L$, this point is algebraic over $K(v)$; and is a generic point of A over K; moreover the intersection product $U\cdot L$ is a prime rational cycle over $K(v)$ having P as a generic point over $K(v)$.*

This lemma is a generalization of Theorem 3 of [WF] Chapter V, Section 1, and follows immediately from that theorem.

Let A^r be a prime rational S^n-cycle over k. Suppose that $\bar{A}$ is not empty, and let $\mathfrak{A}_{11}$ be a component of $\bar{A}$. By Proposition 19, $\mathfrak{A}_{11}$ has the same dimension r as A. We shall define a certain multiplicity which will be denoted by $\mu(A,\mathfrak{A}_{11})$. Let

$$L^{n-r}=(\sum_j t_{ij}X_j-t_i=0\quad(1\leqq i\leqq r))$$

be a generic linear variety [7] over k in S^n; and let

$$\mathfrak{L}^{n-r}=(\sum \tau_{ij}X_j-\tau_i=0\quad(1\leqq i\leqq r))$$

be a generic linear variety over κ, in $\mathfrak{S}^n$. Then we have a point (x) in $L\cap A$, which is a generic point of A over $k(t_{ij})$, and we have a point (ξ) in

[7] By a linear variety $(\sum c_{ij}X_j-c_i=0\ (1\leqq i\leqq r))$ we understand the linear variety defined by the equations $\sum c_{ij}X_j-c_i=0$ $(1\leqq i\leqq r)$. We call it a generic linear variety over K if (c_i,c_{ij}) is a set of independent variables over K.

$\mathfrak{L} \cap \mathfrak{A}_{11}$ which is a generic point of $\mathfrak{A}_{11}$ over $\bar{\kappa}(\tau_{ij})$. The point (x) is algebraic over $k(t_i, t_{ij})$, and (ξ) is algebraic over $\kappa(\tau_i, \tau_{ij})$. Since $\mathfrak{A}_{11}$ is a component of $\bar{A}$, (ξ) is an isolated specialization of (x) over $\mathfrak{o}$. Hence (ξ) is a proper specialization of (x) over $(t_i, t_{ij}) \xrightarrow{\mathfrak{o}} (\tau_i, \tau_{ij})$; so that by Theorem 2 of Section 2, it has a multiplicity μ defined in Section 2. It is easy to see that this multiplicity μ depends only upon the cycle A and the component $\mathfrak{A}_{11}$ of A, and not upon the choices of (t), (τ), (x), and (ξ). We shall denote it by $\mu(A, \mathfrak{A}_{11})$. By Theorem 2, $\mu(A, \mathfrak{A}_{11})$, is a multiple of $[\kappa(\tau_i, \tau_{ij}, \xi) : \kappa(\tau_i, \tau_{ij})]_i$. It can be easily verified that the latter number is equal to the order of inseparability of $\mathfrak{A}_{11}$ over κ.[8] Let $\mathfrak{A}_1$ be the prime rational $\mathfrak{S}^n$-cycle over κ with the component $\mathfrak{A}_{11}$. We denote by $\mu(A, \mathfrak{A}_1)$ the integer $\mu(A, \mathfrak{A}_{11})/[\mathfrak{A}_{11} : \kappa]_i$. It is easy to see that $\mu(A, \mathfrak{A}_1)$ is actually determined only by A and $\mathfrak{A}_1$. We define a $\mathfrak{S}^n$-cycle $\rho(A)$ by $\rho(A) = \sum_\nu \mu(A, \mathfrak{A}_\nu)\mathfrak{A}_\nu$ where the sum is taken over all the prime rational $\mathfrak{S}^n$-cycles $\mathfrak{A}_\nu$ over κ whose components are components of $\bar{A}$. If $\bar{A}$ is empty, we put $\rho(A) = 0$. It is obvious that

$$\rho(A) = \sum_{\nu, i} \mu(A, \mathfrak{A}_{\nu i})\mathfrak{A}_{\nu i}$$

where the sum is taken over all the components $\mathfrak{A}_{\nu i}$ of $\bar{A}$. Let X^r be a rational S^n-cycle over k; and let $X = \sum a_\alpha A_\alpha$ be a representation of X as a linear combination of prime rational S^n-cycles A_α over k. We put $\rho(X) = \sum a_\alpha \rho(A_\alpha)$ and call it the *cycle obtained from X by the reduction with respect to* $\mathfrak{p}$ (or $\mathfrak{o}$). Then, ρ is an additive mapping of the group of rational S^n-cycles over k into the group of rational $\mathfrak{S}^n$-cycles over κ of the same dimension. We shall define in Section 4 such a mapping ρ also for cycles on an abstract variety.

PROPOSITION 20. *Let k' be an extension of k and $\mathfrak{o}'$ a prolongation of $\mathfrak{o}$ in k'. Let X^r be a rational S^n-cycle over k. If we define a cycle $\rho'(X)$ by the same procedure as above, with respect to $\mathfrak{o}'$, then $\rho'(X)$ coincides with $\rho(X)$.*

Proof. By linearity it is sufficient to prove our proposition in case where X is a prime rational cycle A over k. Let $A = \sum a_\alpha A_\alpha$ be a representation of A as a linear combination of prime rational cycles A over k'. Let

$$L^{n-r} = (\sum t_{ij}X_j - t_i = 0 \quad (1 \leqq i \leqq r))$$

be a generic linear variety over k' and

$$\mathfrak{L}^{n-r} = (\sum \tau_{ij}X_j - \tau_i = 0 \quad (1 \leqq i \leqq r))$$

---

[8] We shall denote by $[V: K]_i$ the order of inseparability of the variety V over a field K. If A is a prime rational cycle over K with the component V then we denote it also by $[A: K]_i$.

be a generic linear variety over the residue field κ' of $\mathfrak{o}'$. Let (x) be a point in $L \cap A$ and (ξ) a point in $\mathfrak{L} \cap \mathfrak{A}_{11}$, where $\mathfrak{A}_{11}$ is a component of $\bar{A}$. By Lemma 2, and by the equation $L \cdot A = \sum a_\alpha L \cdot A_\alpha$, the complete set of conjugates of (x) over $k(t_i, t_{ij})$ consists of the complete set of conjugates of $(x^{(\alpha)})$ over $k'(t_i, t_{ij})$, each set being repeated a_α times, where $(x^{(\alpha)})$ is a point in $L \cap A_\alpha$. By counting the number of (ξ) in a specialization of the complete set of conjugates of (x) over $k(t_i, t_{ij})$, over $(t_i, t_{ij}) \xrightarrow{\mathfrak{o}'} (\tau_i, \tau_{ij})$, we have $\mu(A, \mathfrak{A}_{11}) = \sum a_\alpha \mu'(A_\alpha, \mathfrak{A}_{11})$ where μ' is the multiplicity defined with respect to $\mathfrak{o}'$. By Theorem 7, a variety $\mathfrak{A}^r$ in $\mathfrak{S}^n$ is a component of $\rho(A)$ if and only if it is a component of $\rho'(A)$; so our proposition is proved.

PROPOSITION 21. *Let A^r be a prime rational S^n-cycle over k, and $\mathfrak{A}^r$ a prime rational $\mathfrak{S}^n$-cycle over κ with a component in $\bar{A}$. Let*

$$L^{n-r} = (\sum d_{ij}X_j - e_i = 0 \quad (1 \leqq i \leqq r))$$

be a linear variety in S^n, such that all the elements d_{ij} which are not in $\mathfrak{o}$ form a set of independent variables over k and that (e) is a set of independent variables over $k(d)$. Let

$$\mathfrak{L}^{n-r} = (\sum \delta_{ij}X_j - \epsilon_i = 0 \quad (1 \leqq i \leqq r))$$

be a linear variety in $\mathfrak{S}^n$, such that $\kappa(\delta)$ is regular over κ and that (ϵ) is a set of independent variables over $\kappa(\delta)$. Suppose that (δ, ϵ) is a specialization of (d, e) over $\mathfrak{o}$ and that there are a point (x) in $L \cap A$ and a point (ξ) in $\mathfrak{L} \cap \mathfrak{A}$. Then (ξ) is a proper specialization of (x) over $(d, e) \xrightarrow{\mathfrak{o}} (\delta, \epsilon)$, of multiplicity $\mu(A, \mathfrak{A}) \cdot [\kappa(\delta, \epsilon, \xi) : \kappa(\delta, \epsilon)]_i$.

Proof. First we remark that A is prime rational over $k(d)$ and that $\mathfrak{A}$ is prime rational over $\kappa(\delta)$. By Lemma 2, (x) is a generic point of A over $k(d)$ and (ξ) is a generic point of $\mathfrak{A}$ over $\kappa(\delta)$. Now it is obvious that (ξ) is a proper specialization of (x) over $(d, e) \xrightarrow{\mathfrak{o}} (\delta, \epsilon)$, since $(x) \longrightarrow (\xi)$ is isolated over $\mathfrak{o}$. By our assumption for the set (d) and by Theorem 2 of Section 2, (ξ) has a multiplicity μ as a specialization of (x) over $(d, e) \xrightarrow{\mathfrak{o}} (\delta, \epsilon)$. Let

$$M^{n-r} = (\sum t_{ij}X_j - t_i = 0 \quad (1 \leqq i \leqq r))$$

be a generic linear variety over $k(d, e)$ and

$$\mathfrak{M}^{n-r} = (\sum \tau_{ij}X_j - \tau_i = 0 \quad (1 \leqq i \leqq r))$$

a generic linear variety over $\kappa(\delta, \epsilon)$. Then we have a point (y) in $M \cap A$ and a point (η) in $\mathfrak{M} \cap \mathfrak{A}$. Obviously, (η) is also a proper specialization of

(y) over $(t_{ij}, t_i) \xrightarrow{\mathfrak{o}} (\tau_{ij}, \tau_i)$; so that it has a multiplicity μ_1. We shall show $\mu = \mu_1$. Let $(y^{(1)}, \cdots, y^{(m)})$ be the complete set of conjugates of (y) over $k(t)$ and $(x^{(1)}, \cdots, x^{(m)})$ a specialization of $(y^{(1)}, \cdots, y^{(m)})$ over $(t_{ij}, t_i) \xrightarrow{k} (d_{ij}, e_i)$. Then, by Lemma 2 and the definition of intersection-multiplicity,[8'] $(x^{(1)}, \cdots, x^{(m)})$ consists of the complete set of conjugates of (x) over $k(d, e)$ and pseudo-points which may arise or may not arise. Let $(\xi^{(1)}, \cdots, \xi^{(m)})$ be a specialization of $(x^{(1)}, \cdots, x^{(m)})$ over $(d, e) \xrightarrow{\mathfrak{o}} (\delta, \epsilon)$; then we see that (ξ) occurs in $(\xi^{(1)}, \cdots, \xi^{(m)})$ exactly μ times. Thus we have shown $\mu = \mu_1$. Let $(\eta^{(1)}, \cdots, \eta^{(m)})$ be a specialization of $(y^{(1)}, \cdots, y^{(m)})$ over $(t_{ij}, t_i) \xrightarrow{\mathfrak{o}} (\tau_{ij}, \tau_i)$ and $(\xi'^{(1)}, \cdots, \xi'^{(m)})$, a specialization of $(\eta^{(1)}, \cdots, \eta^{(m)})$ over $(\tau_{ij}, \tau_i) \xrightarrow{\kappa} (\delta_{ij}, \epsilon_i)$. By definition of μ_1, we have (ξ) in $(\xi'^{(1)}, \cdots, \xi'^{(m)})$ exactly μ_1 times. If $(\xi'^{(\nu)}) = (\xi)$, then we have

$$(x) \xrightarrow{k} (y^{(\nu)}) \xrightarrow{\mathfrak{o}} (\eta^{(\nu)}) \xrightarrow{\kappa} (\xi).$$

By the isolatedness of $(x) \xrightarrow{\mathfrak{o}} (\xi)$, we have $(\xi) \xrightarrow{\kappa} (\eta^{(\nu)})$, this shows that $(\eta^{(\nu)})$ is in $\mathfrak{A}$. Since $(y^{(\nu)}, t_{ij}, t_i) \xrightarrow{\mathfrak{o}} (\eta^{(\nu)}, \tau_{ij}, \tau_i)$ and since $(y^{(\nu)}) \varepsilon M$, we see that $(\eta^{(\nu)})$ is in $\mathfrak{M} \cap \mathfrak{A}$, so that $(\eta^{(\nu)})$ is a conjugate of (η) over $\kappa(\tau)$. Now by our definition of $\mu(A, \mathfrak{A})$, the complete set of conjugates of (η) occurs in $(\eta^{(1)}, \cdots, \eta^{(m)})$ exactly $\mu(A, \mathfrak{A})$ times. Then, by Lemma 2 and by the definition of intersection-multiplicity, we have $\mu(A, \mathfrak{A})[\kappa(\delta, \epsilon, \xi) : \kappa(\delta, \epsilon)]_i$ = the number of (ξ) which occurs in $(\xi'^{(1)}, \cdots, \xi'^{(m)})$. This completes our proof.

THEOREM 8. *Let A^r be a rational S^m-cycle over k and B^s a rational S^n-cycle over k. Then we have $\rho(A \times B) = \rho(A) \times \rho(B)$.*

Proof. By linearity and by Proposition 20, it is sufficient to prove our theorem in case where A and B are varieties defined over k. Furthermore, we may assume that all the components of $\bar{A}$ and $\bar{B}$ are defined over κ, because for every extension κ' of κ, there exists, by Proposition 9 of Section 1, a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ such that κ' is the residue field of $\mathfrak{o}'$. By Proposition 18, a variety $\mathfrak{C}$ in $\mathfrak{S}^n \times \mathfrak{S}^m$ is a component of $\overline{A \times B}$ if and only if it is a product $\mathfrak{A} \times \mathfrak{B}$ where $\mathfrak{A}$ is a component of $\bar{A}$ and $\mathfrak{B}$ is a component of $\bar{B}$. Hence it suffices to prove $\mu(A \times B, \mathfrak{A} \times \mathfrak{B}) = \mu(A, \mathfrak{A}) \cdot \mu(B, \mathfrak{B})$. Let $M^{m-r} = (\sum t_{ij}X_j - t_i = 0 \ (1 \leqq i \leqq r))$ be a generic linear variety over k in S^m and $N^{n-s} = (\sum z_{ij}X_j - z_i = 0 \ (1 \leqq i \leqq s))$ a generic linear variety over $k(t)$ in S^n. Correspondingly, let $\mathfrak{M}^{m-r} = (\sum \tau_{ij}X_j - \tau_i = 0 \ (1 \leqq i \leqq r))$ be a generic linear variety over κ in $\mathfrak{S}^m$ and $\mathfrak{N}^{n-s} = (\sum \zeta_{ij}X_j - \zeta_i = 0 \ (1 \leqq i \leqq s))$ a generic linear variety over $\kappa(\tau)$ in $\mathfrak{S}^n$. We have points (x),

[8'] See [WF] Chapter V, Section 1.

(y), (ξ) and (η) respectively in $M \cap A$, $N \cap B$, $\mathfrak{M} \cap \mathfrak{A}$ and $\mathfrak{N} \cap \mathfrak{B}$. Applying Proposition 21 to $A \times B$, $\mathfrak{A} \times \mathfrak{B}$, $M \times N$ and $\mathfrak{M} \times \mathfrak{N}$, we see that the multiplicity of (ξ, η) as a specialization of (x, y) over $(t_{ij}, z_{ij}, t_i, z_i) \xrightarrow{\mathfrak{o}} (\tau_{ij}, \zeta_{ij}, \tau_i, \zeta_i)$ is equal to $\mu(A \times B, \mathfrak{A} \times \mathfrak{B})$. By Theorem 4 of Section 2 and by our definition of $\mu(A, \mathfrak{A})$, this multiplicity is equal to $\mu(A, \mathfrak{A}) \cdot \mu(B, \mathfrak{B})$.

Now we consider the relation between our multiplicity $\mu(A, \mathfrak{A})$ and the intersection-multiplicity.

Let U^n be a variety defined over a field K; let A^r and B^s be prime rational U-cycles over K. If there is a component C_1 of the bunch $A \cap B$, which is simple on U and has dimension $r + s - n$, then every conjugate of C_1 over K is also a simple component of $A \cap B$ on U with the dimension $r + s - n$. Consider the number

$$[A:K]_i [B:K]_i [C_1:K]_i^{-1} \sum_{p,q} i(A_p \cdot B_q, C_1; U)$$

where the sum is taken over all the A_p and all the B_q which are respectively components of A and B, and which contains C_1. It is easy to see that this number is invariant when we replace C_1 with any conjugate of C_1 over K. We denote this number by $i_K(A \cdot B, C; U)$ where C is a prime rational U-cycle over K with the component C_1. We shall say that C is a *prime component of* $A \cap B$ on U, over K, if U, A, B and C are in the above situation. We shall also use the notation $j_K(V \cdot L, W)$ for an intersection of a prime rational cycle and a linear variety.

THEOREM 9. *Let V^r be a variety defined over k in S^n. Let*

$$L^{n-s} = (\sum c_{ij} X_j - c_i = 0 \quad (1 \leqq i \leqq s))$$

be a linear variety in S^n where $c_{ij} \in \mathfrak{o}$, $c_i \in \mathfrak{o}$; and let

$$\mathfrak{L}^{n-s} = (\sum \gamma_{ij} X_j - \gamma_i = 0 \quad (1 \leqq i \leqq s))$$

be a linear variety in $\mathfrak{S}^n$ such that $(c_{ij}, c_i) \xrightarrow{\mathfrak{o}} (\gamma_{ij}, \gamma_i)$. If there is a component $\mathfrak{W}_1$ of dimension $r - s$ in $\bar{V} \cap \bar{L}$, then there exists a prime rational cycle W^{r-s} over k with a component in $V \cap L$ such that $\mathfrak{W}_1$ is a component of $\bar{W}$. If we denote by the W_ν such cycles, then for every ν, W_ν is a prime component of $V \cap L$ over k; and we have

$$\sum_\nu j_k(V \cdot L, W_\nu) \mu(W_\nu, \mathfrak{W}) = \sum_\nu \mu(V, \mathfrak{B}_\nu) j_\kappa(\mathfrak{B}_\nu \cdot \mathfrak{L}, \mathfrak{W}),$$

where $\mathfrak{W}$ is the prime rational cycle over κ with the component $\mathfrak{W}_1$, and the $\mathfrak{B}_\nu$ are all the prime components of $\rho(V)$[9] *over κ which contain $\mathfrak{W}_1$.*

---

[9] We understand by a prime component over K, of a rational cycle over K, a prime rational cycle over K with a component which appears in the reduced expression of that rational cycle.

Proof. Let $M^{n-s} = (\sum t_{ij}X_j - t_i = 0 \ (1 \leqq i \leqq s))$ be a generic linear variety over k and $N^{n-r+s} = (\sum z_{ij}X_j - z_i = 0 \ (1 \leqq i \leqq r-s))$ a generic linear variety over $k(t)$. Correspondingly, let $\mathfrak{M}^{n-s} = (\sum \tau_{ij}X_j - \tau_i = 0 \ (1 \leqq i \leqq s))$ be a generic linear variety over κ and $\mathfrak{N}^{n-r+s} = (\sum \zeta_{ij}X_j - \zeta_i = 0 \ (1 \leqq i \leqq r-s))$ a generic linear variety over $\kappa(\tau)$. Then we have a point (x) in $V \cap M \cap N$ and a point (η) in $\mathfrak{W}_1 \cap \mathfrak{N}$. By Lemma 2, (x) is a generic point of V over $k(t_{ij}, z_{ij})$; and (η) is a generic point of $\mathfrak{W}_1$ over $\bar{\kappa}(\zeta_{ij})$. It is easy to see that (η) is a specialization of (x) over $(t_{ij}, t_i, z_{ij}, z_i) \xrightarrow{\mathfrak{o}} (\gamma_{ij}, \gamma_i, \zeta_{ij}, \zeta_i)$. Moreover (η) is an isolated specialization of (x) over $(t_{ij}, t_i) \xrightarrow{\mathfrak{o}} (\gamma_{ij}, \gamma_i)$. For, if $(x, t) \xrightarrow{\mathfrak{o}} (\eta', \gamma) \xrightarrow{\kappa} (\eta, \gamma)$, then (η') is in $\bar{V} \cap \bar{L}$ and has (η) as a specialization over κ. Since (η) is a generic point of a component $\mathfrak{W}_1$ of $\bar{V} \cap \bar{L}$, we have $(\eta) \xrightarrow{\kappa} (\eta')$. Hence (η) is a proper specialization of (x) over $(t, z) \xrightarrow{\mathfrak{o}} (\gamma, \zeta)$, and by Theorem 2 of Section 2, has a multiplicity μ. Now consider a series of specializations $(t, z) \xrightarrow{k} (c, z) \xrightarrow{\mathfrak{o}} (\gamma, \zeta)$. By (I) of Proposition 14 of Section 2, there exists a set (y) such that $(x, t, z) \xrightarrow{k} (y, c, z) \xrightarrow{\mathfrak{o}} (\eta, \gamma, \zeta)$. Since $\sum t_{ij}x_j = t_i \ (1 \leqq i \leqq s)$, we have $\sum c_{ij}y_j = c_i \ (1 \leqq i \leqq s)$; so that (y) is contained in $V \cap L$. Let W_0 be the locus of (y) over k, and W_0' the component of $V \cap L$ which contains W_0. Then we have $\bar{W}' \supset \mathfrak{W}_1$ where W' is the prime rational cycle over k, with the component W_0'. Since $\mathfrak{W}_1$ is a component of $\bar{V} \cap \bar{L}$, $\mathfrak{W}_1$ must be a component of $\bar{W}'$; so that we have $\dim \mathfrak{W}_1 = \dim W' \geqq \dim W_0 \geqq \dim \mathfrak{W}_1$. From this follows that W_0 is a component of $V \cap L$ and that $\dim W_0 = \dim \mathfrak{W}_1$. This proves the existence of a prime rational cycle W over k in our theorem. Let the W_ν be such cycles; then by the same argument as above we have $\dim W_\nu = \dim \mathfrak{W}_1 = r + s - n$; so that the W_ν are prime components of $V \cap L$ over k. Let k' be an extension of k and $\mathfrak{o}'$ a prolongation of $\mathfrak{o}$ in k' such that all the components of $V \cap L$ are defined over k' and that all the components of $\bar{V}$ and $\bar{V} \cap \bar{L}$ are defined over the residue field κ' of $\mathfrak{o}'$.[9'] We denote by $\mu'(A, \mathfrak{A})$ the multiplicity with respect to $\mathfrak{o}'$. Denote by the $W_{\nu\lambda}$ the components of W_ν for every ν and by the $\mathfrak{B}_{\nu\lambda}$ the components of $\mathfrak{B}_\nu$ for every ν. By Proposition 20, we have

$$[\mathfrak{W} : k]_i \sum_\nu j_k(V \cdot L, W_\nu)\mu(W_\nu, \mathfrak{W})$$
$$= \sum_\nu j(V \cdot L, W_{\nu 1})[W_\nu : k]_i^{-1} \sum_\lambda [W_\nu : k]_i \mu'(W_{\nu\lambda}, \mathfrak{W}_1)$$
$$= \sum_{\nu,\lambda} j(V \cdot L, W_{\nu\lambda})\mu'(W_{\nu\lambda}, \mathfrak{W}_1).$$

[9'] The existences of such an extension k' and a prolongation $\mathfrak{o}'$ are assured by Proposition 9 in Section 1.

Similarly we have

$$[\mathfrak{W}:k]_i \sum_\nu \mu(V,\mathfrak{V}_\nu) j_\kappa(\mathfrak{V}_\nu\cdot\mathfrak{L},\mathfrak{W}) = \sum_{\nu,\lambda} \mu'(V,\mathfrak{V}_{\nu\lambda}) j(\mathfrak{V}_{\nu\lambda}\cdot\mathfrak{L},\mathfrak{W}_1).$$

By these equations it suffices to prove the formula in our theorem in case where all the components of $V \cap L$ are defined over k and where all the components of $\bar{V}$ and $\bar{V} \cap \bar{L}$ are defined over κ. Assume that we are in this situation. Let (y') be a point in $W_\nu \cap N$, then (y') is a generic point of W_ν over k; and we have $(x,t,z) \xrightarrow{k} (y',c,z) \xrightarrow{o} (\eta,\gamma,\zeta)$. Conversely if we have $(x,t,z) \xrightarrow{k} (y',c,z) \xrightarrow{o} (\eta,\gamma,\zeta)$, then (y') is a generic point of some W_ν and is contained in $W_\nu \cap N$. This is already proved. Any such two points (y') and (y'') are conjugates of each other over $k(z)$ if and only if the loci of them are the same. Now let $(x^{(1)},\cdots,x^{(d)})$ be the complete set of conjugates of (x) over $k(t,z)$. We extend the specializations $(t,z) \xrightarrow{k} (c,z) \xrightarrow{o} (\gamma,\zeta)$ to specializations

$$(x^{(1)},\cdots,x^{(d)},t,z) \xrightarrow{k} (y^{(1)},\cdots,y^{(d)},c,z) \xrightarrow{o} (\eta^{(1)},\cdots,\eta^{(d)},\gamma,\zeta).$$

If $(\eta^{(\lambda)}) = (\eta)$, then $(y^{(\lambda)})$ is in $W_\nu \cap N$ for some W_ν. By the definition of $j(V\cdot L,W_\nu)$ ([WF] Chapter V, Section 2), we have the complete set of conjugates of $(y^{(\lambda)})$ over $k(z)$ in $(y^{(1)},\cdots,y^{(d)})$, exactly $j(V\cdot L,W_\nu)$ times. Hence we have $\sum_\nu j(V\cdot L,W_\nu)\mu(W_\nu,\mathfrak{W})$ as the number μ of (η) which occurs in $(\eta^{(1)},\cdots,\eta^{(d)})$. We consider another series of specializations $(t,z) \xrightarrow{o} (\tau,\zeta) \xrightarrow{\kappa} (\gamma,\zeta)$. Then a point (ξ) is a generic point of one of the $\mathfrak{V}_\nu$ and is contained in $\mathfrak{M} \cap \mathfrak{N}$ if and only if

$$(x,t,z) \xrightarrow{o} (\xi,\tau,\zeta) \xrightarrow{\kappa} (\eta,\gamma,\zeta).$$

The loci of any such two points (ξ') and (ξ'') are the same if and only if they are conjugates of each other over $\kappa(\tau,\zeta)$. Hence we have as above, $\mu = \sum_\nu \mu(V,\mathfrak{V}_\nu) j(\mathfrak{V}_\nu\cdot\mathfrak{L},\mathfrak{W})$. This completes our proof.

We denote by $j_\kappa(V\cdot\mathfrak{L},\mathfrak{W})$ the number $\sum_\nu \mu(V,\mathfrak{V}_\nu) j_\kappa(\mathfrak{V}_\nu\cdot\mathfrak{L},\mathfrak{W})$ in the above theorem. It is easily verified that the number $j_\kappa(V\cdot\mathfrak{L},\mathfrak{W})[\mathfrak{W}:\kappa]_i$ is equal to the multiplicity of (η) as a specialization of (x) over $(t,z) \xrightarrow{o} (\gamma,\zeta)$ where the notations are the same as in the above proof. We shall also denote by $j(V\cdot\mathfrak{L},\mathfrak{W}_1)$ this number $j_\kappa(V\cdot\mathfrak{L},\mathfrak{W})[\mathfrak{W}:\kappa]_i$ where $\mathfrak{W}_1$ is a component of $\mathfrak{W}$. Using this j, we have $\mu(V,\mathfrak{V}) = j(V\cdot\mathfrak{S}^n,\mathfrak{V})$ for every prime component $\mathfrak{V}$ of $\rho(V)$.

Before we deal with intersections in the general case, we extend the conception of the simple point. Let V^r be a variety defined over k in S^n, and

denote by $\mathfrak{a}$ the ideal $\{F(X) \mid F(X) \in \mathfrak{o}[X], F(a) = 0$ for every $(a) \in V\}$ in $\mathfrak{o}[X]$. We say that a point (α) in $\bar{V}$ is *simple on* V when there exists a set of polynomials $F_i(X)$ $(1 \leqq i \leqq n - r)$ in $\mathfrak{a}$ such that rank $\|\partial F_i/\partial X_j(\alpha)\|$ is equal to $n - r$. We call the linear variety $(\sum \partial F_i/\partial X_j(\alpha)(X_j - \alpha_j) = 0$ $(1 \leqq i \leqq n - r))$ in $\mathfrak{S}^n$ the *tangent linear variety to* V *at* (α). Also we say that a variety $\mathfrak{W}$ contained in $\bar{V}$ is *simple on* V if some point on $\mathfrak{W}$ is simple on V.

The following proposition is proved as in Theorem 5 of [WF] Chapter IV, Section 3.

PROPOSITION 22. *Let V and W be varieties defined over k, respectively in S^n and S^m. Let (α) be a point in $\bar{V}$ and (β) a point in $\bar{W}$. Then the point $(\alpha) \times (\beta)$ is simple on $V \times W$ if and only if (α) is simple on V and (β) is simple on W.*

Let $\mathfrak{A}$ be a variety in $\bar{V}$ and suppose that $\mathfrak{A}$ is simple on V. We shall use the term "*uniformizing set of linear forms for* V *along* $\mathfrak{A}$." We understand, by this term, a set of r linear forms $\Phi_i(X) = \sum \gamma_{ij} X_j$ $(1 \leqq i \leqq r)$ such that the linear variety $(\Phi_i(X) = 0$ $(1 \leqq i \leqq r))$ in $\mathfrak{S}^n$ is of dimension $n - r$ and is transversal to the tangent linear variety to V at some point of $\mathfrak{A}$. This is an analogy of that for the ordinary case in [WF] Chapter IV, Section 6.

THEOREM 10. *Let V^r be a variety in S^n defined over k and (α) a point in $\bar{V}$ which is simple on V. Let $\mathfrak{L}^{n-r} = (\sum \gamma_{ij} X_j - \gamma_i = 0$ $(1 \leqq i \leqq r))$ be a linear variety in $\mathfrak{S}^n$ which is transversal to the tangent linear variety $\mathfrak{T}^r$ to V at (α). Suppose that (α) is rational over κ and that (γ_{ij}, γ_i) is in κ. Then (α) is a component of $\bar{V} \cap \mathfrak{L}$; and we have $j(V \cdot \mathfrak{L}, (\alpha)) = 1$. In particular, this shows that (α) is contained in only one component $\mathfrak{V}$ of $\bar{V}$. Moreover (α) is a simple point on $\mathfrak{V}$; and $\mathfrak{T}$ is the tangent linear variety to $\mathfrak{V}$ at (α).*

Proof. By Theorem 5 of Section 2, and by the same argument as in the proof of Proposition 7 of [WF] Chapter V, Section 1, it can be proved that $j(V \cdot \mathfrak{L}, (\alpha)) = 1$. Then if we denote by $\mathfrak{V}_1, \cdots, \mathfrak{V}_h$ all the components of $\bar{V}$ which contain (α), we have

$$1 = \sum_{\nu=1}^{h} \mu(V, \mathfrak{V}_\nu) j(\mathfrak{V}_\nu \cdot \mathfrak{L}, (\alpha)).$$

Hence h must be equal to 1. The remaining part of our theorem is obvious.

COROLLARY. *Let V be a variety defined over k and $\mathfrak{V}$ a component of* by the above theorem and the proof of it. From this follows $[\mathfrak{V} : \kappa]_i = 1$.

Proof. By our definition, there exists a point (α) on $\mathfrak{B}$ which is simple on V. By Proposition 9 of Section 1, there exist an extension k' of k and a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ in k' such that the residue field of $\mathfrak{o}'$ is $\kappa(\alpha)$. Since $\mu(V, \mathfrak{B})$ is invariant when considered with respect to $\mathfrak{o}'$, we have $\mu(V, \mathfrak{B}) = 1$ by the above theorem and the proof of it. From this follows $[\mathfrak{B} : \kappa]_i = 1$.

THEOREM 11. *Let U^n be a variety defined over k; let A^r and B^r be two prime rational U-cycles over k. Suppose that there exists a component $\mathfrak{C}_1^{r+s-n}$ of $\bar{A} \cap B$ which is simple on U. Then, there exists a prime rational cycle C over k with a component in $A \cap B$ such that $\mathfrak{C}_1$ is a component of $\bar{C}$. If we denote by the C_ν such cycles, then every C_ν is a prime component of $A \cap B$ on U over k. Let the $\mathfrak{A}_p^r$ and the $\mathfrak{B}_q^s$ be those prime rational cycles over κ which contain $\mathfrak{C}_1$, and of which components are components of $\bar{A}$ and $\bar{B}$, respectively; and let $\mathfrak{U}$ be the component of U which contains $\mathfrak{C}_1$ (by Theorem 10, such $\mathfrak{U}$ is uniquely determined), and $\mathfrak{C}$ the prime rational cycle over κ with the component $\mathfrak{C}_1$. If $\mathfrak{U}$ is defined over κ, then, the $\mathfrak{A}_p$ and the $\mathfrak{B}_q$ are all contained in $\mathfrak{U}$; and $\mathfrak{C}$ is a prime component of $\mathfrak{A}_p \cap \mathfrak{B}_q$ on $\mathfrak{U}$ over κ, for every p and q; and we have the following formula:*

$$\sum_{\nu} i_k(A \cdot B, C_\nu; U)\mu(C_\nu, \mathfrak{C}) = \sum_{p,q} \mu(A, \mathfrak{A}_p)\mu(B, \mathfrak{B}_q) i_\kappa(\mathfrak{A}_p \cdot \mathfrak{B}_q, \mathfrak{C}; \mathfrak{U}).$$

Proof. Let k' be an extension of k and $\mathfrak{o}'$ a prolongation of $\mathfrak{o}$ in k' such that all the components of A, B and $A \cap B$ are defined over k', and that all the components of $\bar{A}$, $\bar{B}$ and $\bar{A} \cap \bar{B}$ are defined over the residue field κ' of $\mathfrak{o}'$. We shall denote by $\mu'(A, \mathfrak{A})$ our multiplicity with respect to $\mathfrak{o}'$. Suppose that there exists a component C_0 of $A \cap B$ such that $\bar{C}_0 \supset \mathfrak{C}_1$, and denote by C the prime rational cycle over k with the component C_0. Then, similarly as in the proof of Theorem 9, we can prove that $\mathfrak{C}_1$ is a component of $\bar{C}$ and that C is a prime component of $A \cap B$ on U over k. If we define the C_ν, the $\mathfrak{A}_p$, the $\mathfrak{B}_q$ and $\mathfrak{U}$ as in our theorem, then it is obvious that the $\mathfrak{A}_p$ and the $\mathfrak{B}_q$ are all contained in $\mathfrak{U}$ and that $\mathfrak{C}$ is a prime component of $\mathfrak{A}_p \cap \mathfrak{B}_q$ on $\mathfrak{U}$ over κ. Denote the components of A, B, C_ν, $\mathfrak{A}_p$ and $\mathfrak{B}_q$ respectively by A_α, B_β, $C_{\nu\lambda}$, $\mathfrak{A}_{pu}$ and $\mathfrak{B}_{qv}$. By Proposition 20 and by our definition of $i_k(A \cdot B, C_\nu; U)$, we have

$$[A : k]_i^{-1}[B : k]_i^{-1}[\mathfrak{C} : \kappa]_i \sum_{\nu} i_k(A \cdot B, C_\nu; U)\mu(C_\nu, \mathfrak{C})$$
$$= \sum_{\alpha,\beta,\nu,\lambda} i(A_\alpha \cdot B_\beta, C_{\nu\lambda}; U)\mu'(C_{\nu\lambda}, \mathfrak{C}_1)$$

and

$$[A : k]_i^{-1}[B : k]_i^{-1}[\mathfrak{C} : \kappa]_i \sum_{p,q} \mu(A, \mathfrak{A}_p)\mu(B, \mathfrak{B}_q) i_\kappa(\mathfrak{A}_p \cdot \mathfrak{B}_q, \mathfrak{C}; \mathfrak{U})$$
$$= \sum_{\alpha,\beta,p,q,u,v} \mu'(A_\alpha, \mathfrak{A}_{pu})\mu'(B_\beta, \mathfrak{B}_{qv}) i(\mathfrak{A}_{pu} \cdot \mathfrak{B}_{qv}, \mathfrak{C}_1; \mathfrak{U}).$$

By these equations, it is sufficient to prove our theorem in case where A, B, and the components of $A \cap B$ are all defined over k and where all the components of $\bar{A}$, $\bar{B}$ and $\bar{A} \cap \bar{B}$ are defined over κ. Assume that we are in this case. Let S^N and $\mathfrak{S}^N$ be respectively the ambient spaces for U and $\mathfrak{U}$. Let $\bar{F}_i(X)$ $(1 \leqq i \leqq n)$ be a uniformizing set of linear forms for U along $\mathfrak{C}$. We may assume that for every i, $\bar{F}_i(X)$ is the class of a linear form $F_i(X)$ in $\mathfrak{o}[X]$ modulo $\mathfrak{p}$. We denote by Λ^{2N-n} and $\bar{\Lambda}^{2N-n}$ respectively the linear variety $(F_i(X-X')=0 \ (1 \leqq i \leqq n))$ in $S^N \times S^N$ and the linear variety $(\bar{F}_i(X-X')=0 \ (1 \leqq i \leqq n)$ in $\mathfrak{S}^N \times \mathfrak{S}^N$. Let (γ) be a generic point of $\mathfrak{C}$ over κ and $\Delta_{\mathfrak{C}}$ the locus of (γ, γ) over κ. Then, $\Delta_{\mathfrak{C}}$ is a proper component of $\bar{\Lambda} \cap (\mathfrak{A}_p \times \mathfrak{B}_q)$; and by definition of i ([WF] Chapter VI, Section 1), we have $i(\mathfrak{A}_p \cdot \mathfrak{B}_q, \mathfrak{C}; \mathfrak{U}) = j[(\mathfrak{A}_p \times \mathfrak{B}_q) \cdot \bar{\Lambda}, \Delta_{\mathfrak{C}}]$. By Theorem 9, there exists a component D of $\Lambda \cap (A \times B)$ such that $\bar{D} \supset \Delta_{\mathfrak{C}}$. (We may assume that the components of $\Lambda \cap (A \times B)$ are all defined over k.) If we denote by $D_1, \cdots, D_h$ such components of $\Lambda \cap (A \times B)$, then by the same theorem, we have

$$\sum_{\nu} j[(A \times B) \cdot \Lambda, D_\nu] \mu(D_\nu, \Delta_{\mathfrak{C}}) = \sum_{p,q} \mu(A \times B, \mathfrak{A}_p \times \mathfrak{B}_q) j[(\mathfrak{A}_p \times \mathfrak{B}_q) \cdot \bar{\Lambda}, \Delta_{\mathfrak{C}}].$$

Let (c, c') be a generic point of D over k. Put $k_1 = k(c, c')$. As it is well-known, we can extend the specialization ring $[(c, c') \xrightarrow{\mathfrak{o}} (\gamma, \gamma)]$ to a valuation ring $\mathfrak{o}_1$ in k_1.[9'''] Since $\dim_k (c, c') = \dim_\kappa (\gamma, \gamma)$, $\mathfrak{o}_1$ is discrete. Put

$$L^{N-n} = (F_i(X - c') = 0 \ (1 \leqq i \leqq n)), \quad \mathfrak{L}^{N-n} = \bar{F}_i(X - \gamma) = 0 \ (1 \leqq i \leqq n)).$$

Then, since $\mathfrak{L}$ is transversal to the tangent linear variety to U at (γ), we have, by Theorem 10, $j(U \cdot \mathfrak{L}, (\gamma)) = 1$. If we denote by $(c^{(1)}), \cdots, (c^{(m)})$ the component of $U \cap L$ such that $\overline{(c^{(i)})} = (\gamma)$ (with respect to a prolongation of $\mathfrak{o}_1$ in an extension of k_1), we have, by Theorem 9

$$1 = \sum_{i=1}^{m} j(U \cdot L, (c^{(i)})) \mu((c^{(i)}), (\gamma));$$

so we have $m = 1$ and $j(U \cdot L, (c^{(1)})) = 1$. As the point (c, c') is in Λ, (c) and (c') are both contained in L; the coordinates of (c) and (c') are all in $\mathfrak{o}_1$; and $\overline{(c)} = \overline{(c')} = (\gamma)$. So we must have $(c) = (c')$; this shows that D is the diagonal Δ_C of a variety C which is the locus of (c) over k. It can be easily verified that C is a proper component of $A \cap B$ on U. For every D_ν, we have a variety C_ν such that $D_\nu = \Delta_{C_\nu}$. Conversely, if we have a component C' of $A \cap B$ such that $\overline{C'} \supset \mathfrak{C}$, then it is easily proved that $\Delta_{C'}$ is

[9'''] See Theorem 1 and the remark below that theorem.

a component of $\Lambda \cap (A \times B)$; so C' coincides with one of the C_ν. For every ν, the set of linear forms $F_i(X)$ $(1 \leqq i \leqq n)$ is a uniformizing set of linear forms for U along C_ν since $\bar{C}_\nu \supset \mathfrak{C}$ and since the set $\bar{F}_i(X)$ $(1 \leqq i \leqq n)$ is that for U along $\mathfrak{C}$. So we have $i(A \cdot B, C_\nu; U) = j[(A \times B) \cdot \Lambda, \Delta_{C_\nu}]$. By Theorem 8, we have $\mu(A \times B, \mathfrak{A}_p \times \mathfrak{B}_q) = \mu(A, \mathfrak{A}_p)\mu(B, \mathfrak{B}_q)$. Therefore our theorem will be proved if we show that $\mu(\Delta_{C_\nu}, \Delta_{\mathfrak{C}}) = \mu(C_\nu, \mathfrak{C})$. But this is easily proved by means of Proposition 21.[10]

Now, we shall prove the birational invariance of our multiplicity. Let U be a variety in $S^n \times S^m$ defined over k and U' the projection of U on S^n. Let $(x) \times (y)$ be a generic point of U over k and (α) a point in $\overline{U'}$. We say that U is *finite over* (α) if (y) is finite over $(x) \xrightarrow{\mathfrak{o}} (\alpha)$. Also we say that the projection from U to U' is *regular at* (α) if all the y_j are contained in the specialization ring $[(x) \xrightarrow{\mathfrak{o}} (\alpha)]$. Let k' be an extension of k and $\mathfrak{o}'$ a prolongation of $\mathfrak{o}$ in k'. Then by Proposition 6 of Section 1, U is finite over (α) if and only if U is finite over (α) with respect to $\mathfrak{o}'$. Similarly the projection from U to U' is regular at (α) if and only if that projection is regular at (α) with respect to $\mathfrak{o}'$. Let (β) be a specialization of (α) over κ; then the point (β) is a point in $\overline{U'}$. It is easy to see that if U is finite over (β), U is also finite over (α), and that if the projection from U to U' is regular at (β), it is also regular at (α). So we say that U is finite over a variety in $\overline{U'}$ if U is finite over some point in that variety, and also we say that the projection from U to U' is regular along a variety in $\overline{U'}$ if that projection is regular at some point on that variety.

THEOREM 12. *Let U be a variety in $S^n \times S^m$ defined over k, having the same dimension r as its projection U' on S^n. Suppose that there exists a component $\mathfrak{U}'$ of $\overline{U'}$ such that U is finite over $\mathfrak{U}'$. Then there exists a component of $\bar{U}$ whose projection on $\mathfrak{S}^n$ is $\mathfrak{U}'$. If we denote by the $\mathfrak{U}_\nu$ all such components of $\bar{U}$, then we have*

$$[U : U']\mu(U', \mathfrak{U}') = \sum_\nu \mu(U, \mathfrak{U}_\nu)[\mathfrak{U}_\nu : \mathfrak{U}']$$

Proof. Let $L^{n-r} = (\sum t_{ij}X_j - t_i = 0 \ (1 \leqq i \leqq r))$ be a generic linear variety in S^n over k, and $\mathfrak{L}^{n-r} = (\sum \tau_{ij}X_j - \tau_i = 0 \ (1 \leqq i \leqq r))$ a generic linear variety in $\mathfrak{S}^n$ over κ. Then we have a point (x) in $U' \cap L$ and a point (ξ) in $\mathfrak{U}' \cap \mathfrak{L}$. There exists a point (y) in S^m such that (x, y) is a generic point of U over k. By our assumption, (y) is finite over $(x) \xrightarrow{\mathfrak{o}} (\xi)$. Let (η) be a specialization of (y) over $(x) \xrightarrow{\mathfrak{o}} (\xi)$. Then the locus $\mathfrak{U}$ of

[10] Let $M = (\sum t_{ij}X_j - t_i = 0 \ (1 \leqq i \leqq r + s - n))$ be a generic linear variety in S^N over k and $\mathfrak{M} = (\sum \tau_{ij}X_j - \tau_i = 0 \ (1 \leqq i \leqq r + s - n))$ a generic linear variety in $\mathfrak{S}^N$ over κ. Apply Proposition 21 to Δ_{C_ν}, $\Delta_{\mathfrak{C}}$, $M \times S^N$ and $\mathfrak{M} \times \mathfrak{S}^N$.

(ξ, η) over $\bar{\kappa}$ is contained in U and has the projection on $\mathfrak{S}^n$. If we denote by $(\eta^{(\nu)})$ all the specializations of (η) over $(x) \xrightarrow{0} (\xi)$, then, by Theorem 3 of Section 2, we have

$$\sum \mu_\nu = \mu(U', \mathfrak{U}')[k(t, x, y) : k(t, x)],$$

where μ_ν is the multiplicity of $(\xi, \eta^{(\nu)})$ as a specialization of (x, y) over $(t) \xrightarrow{0} (\tau)$. It is obvious that $[U : U'] = [k(t, x, y) : k(t, x)]$. Applying Proposition 21 to U, $\mathfrak{U}_\nu$, $L \times S^m$ and $\mathfrak{L} \times \mathfrak{S}^m$, we have

$$\mu_\nu = \mu(U, \mathfrak{U}_\nu)[\kappa(\tau, \xi, \eta^{(\nu)}) : \kappa(\tau)]_i[\mathfrak{U}_\nu : \kappa]_i^{-1},$$

if we denote by $\mathfrak{U}_\nu$ the locus of $(\xi, \eta^{(\nu)})$ over $\bar{\kappa}$. We have $\mathfrak{U}_\nu = \mathfrak{U}_\lambda$ if and only if $(\eta^{(\nu)})$ and $(\eta^{(\lambda)})$ are conjugates of each other over $\bar{\kappa}(\xi)$. Hence we have

$$\begin{aligned}[U : U']\mu(U', \mathfrak{U}') \\ = \sum{}' \mu(U, \mathfrak{U}_\nu)[\bar{\kappa}(\xi, \eta^{(\nu)}) : \bar{\kappa}(\xi)]_s[\kappa(\tau, \xi, \eta^{(\nu)}) : \kappa(\tau)]_i[\mathfrak{U}_\nu : \kappa]_i^{-1}.\end{aligned}$$

where the sum is extended over all the components $\mathfrak{U}_\nu$ of $\bar{U}$ having $\mathfrak{U}'$ as their projections on $\mathfrak{S}^n$. This proves our theorem.

The following theorem is a translation of Theorem 15 of [WF] Chapter IV, Section 7 to our case, and can be proved similarly.

THEOREM 13. *Let U be a variety in $S^n \times S^m$ defined over k with the projection U' on S^n. Let $\mathfrak{Z}'$ be a variety in $\overline{U'}$ such that the projection from U to U' is regular along $\mathfrak{Z}'$. Then there is one and only one variety $\mathfrak{Z}$ in $\bar{U}$ with the projection $\mathfrak{Z}'$ on $\mathfrak{S}^n$; $\mathfrak{Z}$ is simple on U if and only if $\mathfrak{Z}'$ is simple on U; and we have $[\mathfrak{Z} : \mathfrak{Z}'] = 1$.*

Let T be a birational correspondence between two varieties V and W, defined over k. Let $\mathfrak{Z}_V$ be a variety in V such that the projection from T to V is regular along $\mathfrak{Z}_V$. Then, by Theorem 13, there is one and only one variety $\mathfrak{Z}$ in $\bar{T}$ with the projection $\mathfrak{Z}_V$ on $\bar{V}$. If the projection from T to W is also regular along the projection $\mathfrak{Z}_W$ of $\mathfrak{Z}$ on W, then we say that T is *biregular along* $\mathfrak{Z}_V$ and *along* $\mathfrak{Z}_W$, and that $\mathfrak{Z}_V$ and $\mathfrak{Z}_W$ are *regularly corresponding varieties in $\bar{V}$ and in $\bar{W}$ by T.*

THEOREM 14. *Let T be a birational correspondence between two varieties V and V', defined over k. Let A^r be a prime rational cycle over k, which is contained in V, and $\mathfrak{A}$ a prime component of $\rho(A)$ over κ. Suppose that T is biregular along a component of $\mathfrak{A}$ and denote by A' and $\mathfrak{A}'$ the cycles respectively corresponding to A and $\mathfrak{A}$ by T. Then $\mathfrak{A}'$ is a prime component of $\rho(A')$ over κ; and we have $\mu(A, \mathfrak{A}) = \mu(A', \mathfrak{A}')$.*

This follows immediately from Theorem 12, Theorem 13 and from Proposition 20.

Now we shall prove the converse of Theorem 10.

THEOREM 15. *Let V^r be a variety in S^n defined over k and (ξ) a point in $\bar{V}$. Then (ξ) is simple on V if and only if (ξ) is contained in only one component $\mathfrak{V}$ of $\bar{V}$, $\mu(V,\mathfrak{V})=1$ and (ξ) is simple on $\mathfrak{V}$. Moreover, if that is so, and if (x) is a generic point of V over k, then the specialization ring $[(x)\xrightarrow{\mathfrak{o}}(\xi)]$ is integrally closed.*

Proof. We have only to prove the direct part. Let the t_{ij} and the s_j $(1\leqq i\leqq r, 1\leqq j\leqq n)$ be $(r+1)n$ independent variables over $k(x)$, let the τ_{ij} and the σ_{ij} be $(r+1)n$ independent variables over $\kappa(\xi)$. Put $y_i=\sum t_{ij}x_j$ and $\eta_i=\sum \tau_{ij}\xi_j$ for $1\leqq i\leqq r$, $z=\sum s_jx_j$ and $\zeta=\sum \sigma_j\xi_j$. Denote by $\mathfrak{L}$ the linear variety $(\sum \tau_{ij}X_j-\eta_i=0\ (1\leqq i\leqq r))$. Since $\mathfrak{L}$ is transversal to the tangent linear variety to $\mathfrak{V}$ at (ξ), we have $j(\mathfrak{V}\cdot\mathfrak{L},(\xi))=1$. By Proposition 9 of Section 1, we can find an extension k_1 of k and a prolongation $\mathfrak{o}_1$ of $\mathfrak{o}$ in k_1 such that the residue field of $\mathfrak{o}_1$ is $\kappa(\xi,\tau)$. We may assume that $k(x,t)$ and k_1 are independent over k. With respect to $\mathfrak{o}_1$, our assumption gives

$$j(V\cdot\mathfrak{L},(\xi))=\mu(V,\mathfrak{V})j(\mathfrak{V}\cdot\mathfrak{L},(\xi))=1,$$

so that (ξ) is a proper specialization of (x) over $(t,y)\xrightarrow{\mathfrak{o}_1}(\tau,\eta)$ of multiplicity 1.[10'] Since $k(x,t)$ and k_1 are linearly disjoint over k, we see that (ξ) is a proper specialization of (x) over $(t,y)\xrightarrow{\mathfrak{o}}(\tau,\eta)$ of multiplicity 1. By Proposition 16 of Section 2, ζ is a proper specialization of z over $(t,s,y)\xrightarrow{\mathfrak{o}}(\tau,\sigma,\eta)$, of multiplicity 1. By the same proposition, we have $k(t,s,y,z)=k(t,s,x)$. Put $k'=k(t,s)$ and $\mathfrak{o}'=[(t,s)\xrightarrow{\mathfrak{o}}(\tau,\sigma)]$. By Proposition 17 of Section 2, the specialization ring $[(y,z)\xrightarrow{\mathfrak{o}'}(\eta,\zeta)]$ is integrally closed, so it contains all the x_j since (x) is finite over this specialization ring by Proposition 16 of Section 2. Let Z be the locus of (x,y,z) over k' and W the locus of (y,z) over k'. Then Z is a birational correspondence between V and W; and the above results shows that (ξ) and (η,ζ) are regularly corresponding points by Z. By Proposition 17 of Section 2, (η,ζ) is simple on W; from this and Theorem 13, follows that (ξ) is simple on V. Moreover we have $[(x)\xrightarrow{\mathfrak{o}'}(\xi)]=[(y,z)\xrightarrow{\mathfrak{o}'}(\eta,\zeta)]$. By this and Proposition 7 of Section 1, $[(x)\xrightarrow{\mathfrak{o}}(\xi)]$ is integrally closed.

COROLLARY 1. *Let V be a variety defined over k and $\mathfrak{V}$ a component of $\bar{V}$. Then $\mathfrak{V}$ is simple on V if and only if $\mu(V,\mathfrak{V})=1$.*

[10'] Note that the linear variety $(\sum t_{ij}X_j-y_i=0\ (1\leqq i\leqq r))$ is generic over k and see the remark below the proof of Theorem 9.

This is an immediate consequence of the above theorem and the corollary of Theorem 10.

COROLLARY 2. *Let U be a variety defined over k and $\mathfrak{U}$ a component of $\bar{U}$; let (x) and (ξ) be respectively a generic point of U over k and a generic point of $\mathfrak{U}$ over $\bar{\kappa}$; and denote by $\mathfrak{R}$ the specialization ring $[(x) \xrightarrow{\mathfrak{o}} (\xi)]$. If $\mathfrak{U}$ is simple on U, then the maximal ideal of $\mathfrak{R}$ is the ideal $\mathfrak{p}\mathfrak{R}$.*

Proof. Let the t_{ij} $(1 \leqq i \leqq r+1, 1 \leqq j \leqq n)$ be $(r+1)n$ independent variables over $k(x)$ and the τ_{ij} $(1 \leqq i \leqq r+1, 1 \leqq j \leqq n)$ be $(r+1)n$ independent variables over $\kappa(\xi)$. By Proposition 9 of Section 1, we can find a finite algebraic extension k_1 of k and a prolongation $\mathfrak{o}_1$ of $\mathfrak{o}$ in k_1 such that $\mathfrak{U}$ is defined over the residue field κ_1 of $\mathfrak{o}_1$. We may assume that the maximal ideal $\mathfrak{p}_1$ of $\mathfrak{o}_1$ is the ideal $\mathfrak{p}\mathfrak{o}_1$.[10''] Put $\mathfrak{o}' = [(t) \xrightarrow{\mathfrak{o}_1} (\tau)]$, $\mathfrak{p}' = \mathfrak{p}_1\mathfrak{o}'$, $\kappa' = \kappa_1(\tau)$, $y_i = \sum t_{ij}x_j$ for $1 \leqq i \leqq r+1$ and $\eta_i = \sum \tau_{ij}\xi_j$ for $1 \leqq i \leqq r+1$. Then as in the proof of Theorem 15, we have $[(x) \xrightarrow{\mathfrak{o}'} (\xi)] = [(y) \xrightarrow{\mathfrak{o}'} (\eta)]$. Moreover, if we denote by V the locus of (y) over $k(t)$, then (η) is a point in $\bar{V}$ and it is simple on V. Let $F(Y) = 0$ be an irreducible equation for (y) over $k(t)$ and $\bar{F}_0(Y) = 0$ an irreducible equation for (η) over κ'. We may assume that $F(Y)$ is a primitive polynomial in $\mathfrak{o}'[Y]$ and that $\bar{F}_0(Y)$ is the class of a ploynomial $F_0(Y)$ in $\mathfrak{o}'[Y]$ modulo $\mathfrak{p}'$. We have $\bar{F}(Y) = \bar{F}_0(Y)\bar{F}_1(Y)$ where $\bar{F}_1(Y)$ is a polynomial in $\kappa'[Y]$. Since (η) is simple on V, we have $\partial\bar{F}/\partial Y_j(\eta) \neq 0$ for some j; so that we have $\bar{F}_1(\eta) \neq 0$. Let z be a quantity in $k(x)$ contained in the maximal ideal of $[(x) \xrightarrow{\mathfrak{o}} (\xi)]$. Then we have an expression $z = P(y)/Q(y)$ where $P(Y)$ and $Q(Y)$ are polynomials in $\mathfrak{o}'[Y]$, $\bar{P}(\eta) = 0$ and $\bar{Q}(\eta) \neq 0$. Since $\bar{F}_0(Y) = 0$ is an irreducible equation for (η) over κ', we have $\bar{P}(Y) = \bar{F}_0(Y)\bar{G}(Y)$ where $\bar{G}(Y)$ is a polynomial in $\kappa'[Y]$. Then we have $\bar{P}(Y)\bar{F}_1(Y) = \bar{F}(Y)\bar{G}(Y)$. Let $F_1(Y)$ and $G(Y)$ be polynomials in $\mathfrak{o}'[Y]$ such that $\bar{F}_1(Y)$ and $\bar{G}(Y)$ are respectively the class of $F_1(Y)$ and the class of $G(Y)$ modulo $\mathfrak{p}'$. Then we have

$$P(Y)F_1(Y) = F(Y)G(Y) + \pi H(Y),$$

where $H(Y)$ is a polynomial in $\mathfrak{o}'[Y]$ and π is a prime element of $\mathfrak{o}$. Substituting (y) for (Y), we have $P(y)F_1(y) = \pi H(y)$, so we have $z/\pi = H(y)/[Q(y)F_1(y)]$. Since $\bar{Q}(\eta)\bar{F}_1(\eta) \neq 0$, z/π is contained in $[(y) \xrightarrow{\mathfrak{o}'} (\eta)]$, so in $[(x) \xrightarrow{\mathfrak{o}'} (\xi)]$. Then by Proposition 7 of Section 1, z/π is contained in $[(x) \xrightarrow{\mathfrak{o}} (\xi)]$. This proves our corollary.

[10''] This is assured since we can take k_1 and $\mathfrak{o}_1$ in such a way that $[k_1 : k] = [\kappa_1 : \kappa]$ as in the proof of Proposition 9.

4. Reduction of abstract varieties. Let $[V_\alpha; F_\alpha; T_{\beta\alpha}]$ be an abstract variety in Weil's sense, defined over k; let, for each α, $\mathfrak{F}_\alpha$ be a bunch in $\bar{V}_\alpha$ which is normally algebraic over κ and which contains $\bar{F}_\alpha$. We call the system $[V_\alpha; F_\alpha; \mathfrak{F}_\alpha; T_{\beta\alpha}]$ *a* $\mathfrak{p}$*-variety defined over* k *having* $[V_\alpha; F_\alpha; T_{\beta\alpha}]$ *as its underlying abstract variety* if the following condition is satisfied.

Whenever, for any α *and* β, $\bar{P}_\alpha$ *is a point in* $\bar{V}_\alpha - \mathfrak{F}_\alpha$ *and* $\bar{P}_\beta$ *a point in* $\bar{V}_\beta - \mathfrak{F}_\beta$, *such that* $(\bar{P}_\alpha, \bar{P}_\beta)$ *is in* $\bar{T}_{\beta\alpha}$, *then* $\bar{P}_\alpha$ *and* $\bar{P}_\beta$ *are regularly corresponding points by* $T_{\beta\alpha}$.

We can easily prove the following facts.

i) Let $[V_\alpha; F_\alpha; \mathfrak{F}_\alpha; T_{\beta\alpha}]$ be a $\mathfrak{p}$-variety defined over k and

$$[U_{\alpha_\lambda}; F_{\alpha_\lambda} \cap U_{\alpha_\lambda}; R_{\mu\lambda}]$$

a subvariety of the abstract variety $[V_\alpha; F_\alpha; T_{\beta\alpha}]$. Then the system

$$[U_{\alpha_\lambda}; F_{\alpha_\lambda} \cap U_{\alpha_\lambda}; \mathfrak{F}_{\alpha_\lambda} \cap \bar{U}_{\alpha_\lambda}; R_{\mu\lambda}]$$

defines a $\mathfrak{p}$-variety which will be called a *subvariety* of the $\mathfrak{p}$-variety

$$[V_\alpha; F_\alpha; \mathfrak{F}_\alpha; T_{\beta\alpha}].$$

ii) Let $[V_\alpha; F_\alpha; \mathfrak{F}_\alpha; T_{\beta\alpha}]$ and $[W_\lambda; G_\lambda; \mathfrak{G}_\lambda; S_{\mu\lambda}]$ be two $\mathfrak{p}$-varieties defined over k and $[V_\alpha \times W_\lambda; H_{\alpha\lambda}; U_{\beta\mu,\alpha\lambda}]$ the product-variety of the abstract varieties $[V_\alpha; F_\alpha; T_{\beta\alpha}]$ and $[W_\lambda; G_\lambda; S_{\mu\lambda}]$. Put

$$\mathfrak{H}_{\alpha\lambda} = (\mathfrak{F}_\alpha \times \bar{W}_\lambda) \cup (\bar{V}_\alpha \times \mathfrak{G}_\lambda).$$

Then the system $[V_\alpha \times W_\lambda; H_{\alpha\lambda}; \mathfrak{H}_{\alpha\lambda}; U_{\beta\mu,\alpha\lambda}]$ defines a $\mathfrak{p}$-variety which will be called the *product-variety* of $[V_\alpha; F_\alpha; \mathfrak{g}_\alpha; T_{\beta\alpha}]$ and $[W_\lambda; G_\lambda; \mathfrak{G}_\lambda; S_{\mu\lambda}]$.

iii) The projective space of any dimension defines a $\mathfrak{p}$-variety with the empty $\mathfrak{F}_\alpha$; so that every projective variety defines a uniquely determined $\mathfrak{p}$-variety with the empty $\mathfrak{F}_\alpha$.

Let $[V] = [V_\alpha; F_\alpha; \mathfrak{F}_\alpha; T_{\beta\alpha}]$ be a $\mathfrak{p}$-variety defined over k. Let the M_α be corresponding generic points of the V_α over k by the $T_{\beta\alpha}$ and $(\bar{P}_1, \cdots, \bar{P}_h)$ be any specialization of $(M_1, \cdots, M_h)$ over $\mathfrak{o}$. Similarly as in [WF] p. 168, by a *full set of representatives attached to* $[\bar{V}]$, we understand the set $(\bar{P}_{\alpha_1}, \cdots, \bar{P}_{\alpha_t})$ of all the $\bar{P}_\alpha$ which is finite and not in $\mathfrak{F}_\alpha$. Also we say that $[V]$ is $\mathfrak{p}$*-complete* if no full set of representatives attached to $[\bar{V}]$ is empty. The following facts are easily proved; i) the underlying abstract variety of a $\mathfrak{p}$-complete $\mathfrak{p}$-variety is complete; ii) every subvariety of a $\mathfrak{p}$-complete $\mathfrak{p}$-variety is $\mathfrak{p}$-complete; iii) the product of $\mathfrak{p}$-complete $\mathfrak{p}$-varieties is $\mathfrak{p}$-complete; iv) every projective variety defines a $\mathfrak{p}$-complete $\mathfrak{p}$-variety.

Let $[V]$ be the same as above, and let $[\mathfrak{W}] = [\mathfrak{W}_\lambda; \mathfrak{G}_\lambda; \mathfrak{S}_{\mu\lambda}]$ be an abstract variety defined over an extension field κ' of κ. We say that $[\mathfrak{W}]$ is a *variety in* $[\bar{V}]$ if the following conditions are satisfied: i) there exists a full set of representatives $(\bar{P}_{\alpha_1}, \cdots, P_{\alpha_l})$ attached to $[\bar{V}]$ such that, for every λ, $\mathfrak{W}_\lambda$ is the locus of $\bar{P}_{\alpha_\lambda}$ over κ'; ii) $\mathfrak{G}_\lambda = \mathfrak{W}_\lambda \cap \mathfrak{F}_{\alpha_\lambda}$; iii) $\mathfrak{S}_{\mu\lambda}$ is the variety in $\bar{T}_{\alpha_\mu\alpha_\lambda}$ with the projections $\mathfrak{W}_\lambda$ on $\bar{V}_{\alpha_\lambda}$ and $\mathfrak{W}_\mu$ on $\bar{V}_{\alpha_\mu}$. We call $\mathfrak{W}_\lambda$ the *representative of* $[\mathfrak{W}]$ *in* V_{α_λ}. We can easily prove that for any variety $\mathfrak{W}_\alpha$ in $\bar{V}_\alpha$ which is not contained in $\mathfrak{F}_\alpha$ there is one and only one variety $[\mathfrak{W}]$ in $[\bar{V}]$ such that $\mathfrak{W}_\alpha$ is a representative of $[\mathfrak{W}]$ in V_α. By a *point in* $[\bar{V}]$ we understand a zero-dimensional variety in $[\bar{V}]$. It is obvious that all the representatives of a point in $[\bar{V}]$ forms a full set of representatives attached to $[\bar{V}]$ and conversely. Let $[P]$ be a point in $[V]$ and $[\mathfrak{P}]$ a point in $[\bar{V}]$. We say that $[\mathfrak{P}]$ is a *specialization of* $[P]$ *over* $\mathfrak{o}$ (on $[V]$) if $[P]$ and $[\mathfrak{P}]$ have in some representative V_α of $[V]$, representatives P_α and $\mathfrak{P}_\alpha$ such that $\mathfrak{P}_\alpha$ is a specialization of P_α over $\mathfrak{o}$. We say that a variety $[\mathfrak{W}]$ in $[\bar{V}]$ is *simple on* $[\bar{V}]$ if a representative $\mathfrak{W}_\alpha$ of $[\mathfrak{W}]$ is simple on V_α. We call a finite set of varieties in $[\bar{V}]$ a *bunch in* $[\bar{V}]$; we may identify a bunch with the point-set in $[\bar{V}]$ attached to that bunch. Also, we say that a variety $[\mathfrak{W}]$ is a *component of* a bunch in $[\bar{V}]$ if $[\mathfrak{W}]$ is maximal in that bunch. These definitions are analogies of the definitions in [WF] Chapter VII.

Now our theory of the reduction with respect to $\mathfrak{p}$ can be extended to abstract varieties on which $\mathfrak{p}$-varieties are defined.

Let $[V]$ be a $\mathfrak{p}$-variety defined over k. Let $[A]^r$ be a prime rational $[V]$-cycle over k (which means a prime rational cycle on the underlying abstract variety of $[V]$). We denote by $[\bar{A}]$ the set of all the points in $[\bar{V}]$ which are specializations of some points in $[A]$, over $\mathfrak{o}$. Now we may consider the notation $[\bar{V}]$ in this sense. It is easy to see that the set $[\bar{A}]$ defines a bunch in $[\bar{V}]$. If $[\bar{A}]$ is not empty, then, by Proposition 19 of Section 3, every component of $[\bar{A}]$ is of dimension r. Let $[\mathfrak{A}]_1$ be a component of $[\bar{A}]$. By our definition of $[\bar{A}]$, there exists a representative V_α in which $[A]$ and $[\mathfrak{A}]_1$ have representatives A_α and $\mathfrak{A}_{1\alpha}$.[10] By Theorem 14, of Section 3, the multiplicity $\mu(A_\alpha, \mathfrak{A}_{1\alpha})$ is independent of the choice of representation V_α, A_α, $\mathfrak{A}_{1\alpha}$ for $[V]$, $[A]$ and $[\mathfrak{A}]_1$. We shall denote it by $\mu([A], [\mathfrak{A}]_1)$. Now the results in Section 3 are all translated to the corresponding results on abstract varieties. We shall state them in the following theorems for varieties with a property which we shall call $\mathfrak{p}$-simplicity. We

[10] We shall use the term "representative" also for a prime rational cycle.

shall say that a $\mathfrak{p}$-variety $[V]$ is *$\mathfrak{p}$-simple* if there exists only one component $[\mathfrak{V}]$ in $[\bar{V}]$ and if $\mu([V], [\mathfrak{V}]) = 1$; and we shall call this $[\mathfrak{V}]$ the *abstract variety obtained from $[V]$ by the reduction with respect to $\mathfrak{p}$.*

THEOREM 16. *Let $[V]$ be a $\mathfrak{p}$-simple $\mathfrak{p}$-variety defined over k, then the abstract variety $[\mathfrak{V}]$ obtained from $[V]$ by the reduction with respect to $\mathfrak{p}$ is defined over κ; and a point on $[\mathfrak{V}]$ is simple on $[\mathfrak{V}]$ if and only if it is simple on $[V]$.*

Proof. As for the first assertion, it is sufficient to prove that every representative of $[\mathfrak{V}]$ is defined over κ. Let V_α be a representative of $[V]$ and $\mathfrak{V}_\alpha$ a representative of $[\mathfrak{V}]$ in V_α. By Corollary 1 of Theorem 15 of Section 3 and by corollary of Theorem 10 of Section 3, we have $[\mathfrak{V}_\alpha : \kappa]_i = 1$. This shows $[\kappa' : \kappa]_i = 1$ if we denote by κ' the smallest field of definition for $\mathfrak{V}_\alpha$ which contains κ. Since the bunch $\mathfrak{F}_\alpha$ in $\bar{V}_\alpha$ is normally algebraic over κ, every conjugate of $\mathfrak{V}_\alpha$ over κ is not contained in $\mathfrak{F}_\alpha$; so that, by our assumption, there is no conjugate of $\mathfrak{V}_\alpha$ over κ other than $\mathfrak{V}_\alpha$ itself; so we have $[\kappa' : \kappa]_s = 1$. Hence we have $\kappa' = \kappa$. The remaining part of the theorem follows immediately from Theorem 15 of Section 3.

PROPOSITION 23. *If $[U]$ and $[V]$ are $\mathfrak{p}$-simple $\mathfrak{p}$-varieties defined over k, then the product-variety $[U] \times [V]$ is also $\mathfrak{p}$-simple.*

This is easily proved since the result corresponding to Proposition 5 of [WF] Chapter VII, Section 3 also holds in our case.

Let $[V]$ be a $\mathfrak{p}$-simple variety defined over k and $[\mathfrak{V}]$ the abstract variety obtained from $[V]$ by the reduction with respect to $\mathfrak{p}$. Then every "variety in $[\bar{V}]$" is a subvariety of $[\mathfrak{V}]$. Thus we are able to define the reduction of $[V]$-cycles. Let $[A]^r$ be a prime rational $[V]$-cycle over k and $[\mathfrak{A}]_1{}^r$ a prime rational $[\mathfrak{V}]$-cycle over κ with a component $[\mathfrak{A}]_{11}$ which is a component of $[\bar{A}]$. We denote by $\mu([A], [\mathfrak{A}]_1)$ the number

$$\mu([A], [\mathfrak{A}]_{11})/[[\mathfrak{A}]_{11} : \kappa]_i,$$

and define the $[\mathfrak{V}]$-cycle $\rho([A])$ as follows:

$$\rho([A]) = \sum_\nu \mu([A], [\mathfrak{A}]_\nu)[\mathfrak{A}]_\nu,$$

where the sum is taken over all the prime rational $[\mathfrak{V}]$-cycles $[\mathfrak{A}]_\nu$ over κ with the components which are components of $[\bar{A}]$. Even if $[\bar{A}]$ is not empty the cycle $\rho([A])$ vanishes when every component of $[\bar{A}]$ is not simple on $[\mathfrak{V}]$. Let $[X]$ be a rational $[V]$-cycle over k; we have an expression $[X] = \sum_\lambda a_\lambda [A]_\lambda$ where, for every λ, $[A]_\lambda$ is a prime rational $[V]$-cycle over k. We put

$\rho([X]) = \sum_\lambda a_\lambda \rho([A]_\lambda)$ and call it the *cycle obtained from* $[X]$ *by the reduction with respect to* $\mathfrak{p}$. It is obvious that ρ is a linear mapping of the group of rational $[V]$-cycles over k into the group of rational $[\mathfrak{V}]$-cycles over κ. Similarly as in the affine space, $\rho([X])$ is invariant under the extension of the basic field k and the prolongation of $\mathfrak{o}$. It should be mentioned that the mapping ρ is defined with reference to the ambient variety $[V]$. But we shall use the same notation ρ for mappings of cycles on different ambient varieties, since there will be no confusion.

THEOREM 17. *Let* $[V]$ *be a* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-variety defined over* k. *Let* $[X]^r$ *and* $[Y]^s$ *be positive rational* $[V]$*-cycles over* k *such that the intersection-products* $[X]\cdot[Y]$ *and* $\rho([X])\cdot\rho([Y])$ *are both defined. Then we have* $\rho([X]\cdot[Y]) = \rho([X])\cdot\rho([Y])$.

Proof. By linearity it is sufficient to prove our theorem in case where $[X]$ and $[Y]$ are prime rational $[V]$-cycles $[A]^r$ and $[B]^s$ over k, respectively. Moreover we may assume that $[A]$ and $[B]$ are both varieties defined over k. For, we may take a suitable extension of k and a prolongation of $\mathfrak{o}$ instead of k and $\mathfrak{o}$, since ρ is invariant under such a change of the basic field and ring. We may also assume that every component of $[A]\cap[B]$ is defined over k. Now denote by $[\mathfrak{V}]$ the abstract variety obtained from $[V]$ by reduction. Let $[C]$ be a proper component of $[A]\cap[B]$ on $[V]$ and $[\mathfrak{C}]$ a component of $[\bar{C}]$. If $[\mathfrak{C}]$ is simple on $[\mathfrak{V}]$, it is a component of $\rho([A])\cdot\rho([B])$. To see this let $[\mathfrak{C}]'$ be a component of $[\bar{A}]\cap[\bar{B}]$ containing $[\mathfrak{C}]$; then $[\mathfrak{C}]'$ is simple on $[\mathfrak{V}]$. By our assumption that $\rho([A])\cdot\rho([B])$ is defined on $[\mathfrak{V}]$, we have $\dim[\mathfrak{C}]' = r+s-n$ where n is the dimension of $[V]$ and of $[\mathfrak{V}]$; so that we have $\dim[\mathfrak{C}]' = \dim[C] = \dim[\mathfrak{C}]$. Hence $[\mathfrak{C}]$ is a component of $\rho([A])\cdot\rho([B])$. Conversely, let $[\mathfrak{C}]$ be a component of $\rho([A])\cdot\rho([B])$. Then it is a component of $[\bar{A}]\cap[\bar{B}]$ of dimension $r+s-n$ and is simple on $[\mathfrak{V}]$. By Theorem 16, $[\mathfrak{C}]$ is also simple on $[V]$; then, by Theorem 11 of Section 3, there exists a component $[C]$ of $[A]\cap[B]$ such that $[\mathfrak{C}]$ is a component of $[C]$. Hence we see that $[\mathfrak{C}]$ is a component of $\rho([A]\cdot[B])$. Thus we have proved that a variety on $[\mathfrak{V}]$ is a component of $\rho([A]\cdot[B])$ if and only if it is a component of $\rho([A])\cdot\rho([B])$. Now our theorem is an immediate consequence of the formula in Theorem 11 of Section 3.

THEOREM 18. *Let* $[U]$ *and* $[V]$ *be* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-varieties defined over* k. *If* $[X]$ *is a rational* $[U]$*-cycle over* k *and* $[Y]$ *is a rational* $[V]$*-cycle over* k, *then we have* $\rho([X]\times[Y]) = \rho([X])\times\rho([Y])$.

This follows immediately from Theorem 8 of Section 3 and from our definition of ρ.

THEOREM 19. *Let $[U]$ and $[V]$ be $\mathfrak{p}$-simple $\mathfrak{p}$-varieties defined over k; and let $[\mathfrak{U}]$ and $[\mathfrak{V}]$ be respectively the abstract varieties obtained from $[U]$ and $[V]$ by the reduction with respect to $\mathfrak{p}$. Suppose that $[V]$ is $\mathfrak{p}$-complete and that $[\mathfrak{V}]$ has no multiple point. If $[X]$ is a rational $[U]\times[V]$-cycle over k, then we have $\rho\{\mathrm{pr}_{[U]}([X])\}=\mathrm{pr}_{[\mathfrak{U}]}\{\rho([X])\}$.*

Proof. By linearity, it is enough to prove our theorem in case where $[X]$ is a prime rational cycle $[A]$. Moreover, as in the proof of Theorem 17, we may assume that $[A]$ is a variety defined over k. Let $[A]'$ be the projection of $[A]$ on $[U]$, and $[P]\times[Q]$ a generic point of $[A]$ over k. Our theorem is obvious when $\dim[A]'<\dim[A]$; so we assume that $[A]'$ has the same dimension r as $[A]$ and put $[[A]:[A]']=d$. Let $[\mathfrak{A}]'$ be a component of $\rho([A]')$ and $[\bar{P}]$ a generic point of $[\mathfrak{A}]'$ over $\bar{\kappa}$. Since $[V]$ is $\mathfrak{p}$-complete, there exists a point $[\bar{Q}]$ on $[\mathfrak{V}]$ which is a specialization of $[Q]$ over $[P]\xrightarrow{\mathfrak{o}}[\bar{P}]$. If we denote by $[\mathfrak{A}]$ the locus of $[\bar{P}]\times[\bar{Q}]$ over $\bar{\kappa}$, then $[\mathfrak{A}]$ is a component of $\rho([A])$ with the projection $[\mathfrak{A}]'$ on $[\mathfrak{U}]$. Thus every component of $\rho\{\mathrm{pr}_{[U]}([A])\}$ is a component of $\mathrm{pr}_{[\mathfrak{U}]}\{\rho([A])\}$. It is easy to see that the converse is also true. Now we may assume that the components of $\rho([A])$ and $\rho([A]')$ are all defined over κ. Our theorem is proved when we show that, for every component $[\mathfrak{A}]'$ of $\rho([A]')$,

$$d\cdot\mu([A]',[\mathfrak{A}]')=\sum_{\sigma}\mu([A],[\mathfrak{A}]_\sigma)[[\mathfrak{A}]_\sigma:[\mathfrak{A}]'],$$

where the sum is taken over every component $[\mathfrak{A}]_\sigma$ of $\rho([A])$ with the projection $[\mathfrak{A}]'$ on $[\mathfrak{U}]$. Let U, $\mathfrak{U}$, A', $\mathfrak{A}'$, P, P be representations of $[U]$, $[\mathfrak{U}]$, $[A]'$ $[\mathfrak{A}]'$, $[P]$ and $[\bar{P}]$, respectively; and let S^N and $\mathfrak{S}^N$ be respectively the ambient spaces for U and for $\mathfrak{U}$. We may assume that $[U]=U$ and $[\mathfrak{U}]=\mathfrak{U}$. Let $L^{N-r}=(\sum t_{ij}X_j-t_i=0\ (1\leqq i\leqq r))$ be a generic linear variety in S^N over k and $\mathfrak{L}^{N-r}=(\sum\tau_{ij}X_j-\tau_i=0\ (1\leqq i\leqq r))$ a generic linear variety in $\mathfrak{S}^N$ over κ. We may assume that the point P is in L and that $\bar{P}$ is in $\mathfrak{L}$. Denote by $(P_1,\cdots,P_\delta)$ the complete set of conjugates of P over $k(t)$ and denote by $([Q]_1,\cdots,[Q]_d)$ the complete set of conjugates of $[Q]$ over $k(P)$; then we have the set of δd points $P_\lambda\times[Q]_{\lambda\nu}$ $(1\leqq\lambda\leqq\delta,1\leqq\nu\leqq d)$ as the complete set of conjugates of $P\times[Q]$ over $k(t)$, where $([Q]_{\lambda 1},\cdots,[Q]_{\lambda d})$ is the transform of $([Q]_1,\cdots,[Q]_d)$ by some automorphism over $k(t)$ of $\overline{k(t)}$. Let $(\bar{P}_\lambda\times[\bar{Q}]_{\lambda\nu})$ be a specialization of $(P_\lambda\times[Q]_{\lambda\nu})$ over $(t)\xrightarrow{\mathfrak{o}}(\tau)$. By our assumption that $[V]$ is $\mathfrak{p}$-complete, $[\bar{Q}]_{\lambda\nu}$ is a point of $[\mathfrak{V}]$ for every (λ,ν). If $\bar{P}_\lambda$ is a conjugate of $\bar{P}$

over $\kappa(\tau)$, then $\bar{P}_\lambda \times [\bar{Q}]_{\lambda\nu}$ is a generic point of one of the $[\mathfrak{A}]_\sigma$, say $[\mathfrak{A}]_1$, over κ. If $[\mathfrak{A}]_1$ has a representative in $U \times V_\alpha$ then every generic point of $[\mathfrak{A}]_1$ over κ has a representative in $U \times V_\alpha$. Hence we may consider that we are in the affine space; so that by Proposition 21 of Section 3,[11] the number of (λ, ν) such that $\bar{P}_\lambda \times [\bar{Q}]_{\lambda\nu}$ is a generic point of $[\mathfrak{A}]_1$ over k is equal to $\mu([A], [\mathfrak{A}]_1)[\kappa(\bar{P}_\lambda \times [\bar{Q}]_{\lambda\nu}, \tau) : \kappa(\tau)]$. On the other hand, the number of $\bar{P}_\lambda \times [\bar{Q}]_{\lambda\nu}$ such that $\bar{P}_\lambda$ is a conjugate of $\bar{P}$ over $\kappa(\tau)$ is equal to

$$d \cdot \mu([A]', [\mathfrak{A}]')[\kappa(\bar{P}, \tau) : \kappa(\tau)].$$

Hence we have

$$d \cdot \mu([A]', [\mathfrak{A}]')[\kappa(\bar{P}, \tau) : \kappa(\tau)] = \sum_\sigma \mu([A], [\mathfrak{A}]_\sigma)[[\mathfrak{A}]_\sigma : [\mathfrak{A}]'][\kappa(\bar{P}, \tau) : \kappa(\tau)].$$

This completes our proof.

PROPOSITION 24. *Let $[V]$ be a $\mathfrak{p}$-simple $\mathfrak{p}$-variety defined over k and $[\mathfrak{V}]$ the abstract variety obtained from $[V]$ by the reduction with respect to $\mathfrak{p}$. Suppose that $[V]$ is $\mathfrak{p}$-complete and $[\mathfrak{V}]$ has no multiple point. Then for every rational $[V]$-cycle $[X]$ over k, of dimension* 0, *we have*

$$\deg([X]) = \deg \{\rho([X])\}.$$

Proof. As in the proof of Theorem 17, we may assume that every component of $[X]$ is rational over k. Since every rational point over k has a uniquely determined specialization over $\mathfrak{o}$, our proposition is an immediate consequence of our definition of ρ.

PROPOSITION 25. *Let $[L]^n$ be the projective space defined over k and $[X]$ a rational $[L]$-cycle over k. Consider the abstract variety obtained from $[L]$ by the reduction as the projective space $[\mathfrak{L}]^n$ defined over κ. Then we have* $\deg([X]) = \deg \{\rho([X])\}$.

This follows immediately from Theorem 17 and Proposition 24.

Let $[V]$ be a $\mathfrak{p}$-simple $\mathfrak{p}$-variety defined over k and $[\mathfrak{V}]$ the abstract variety obtained from $[V]$ by the reduction with respect to $\mathfrak{p}$. We denote by $\boldsymbol{F}$ the field of algebraic functions on $[V]$ defined over k and by Φ the field of algebraic functions on $[\mathfrak{V}]$ defined over κ. Let $[P]$ be a generic point of $[V]$ over k and $[\bar{P}]$ a generic point of $[\mathfrak{V}]$ over κ. Let ϕ be an element of $\boldsymbol{F}$ which is defined by $z = \phi([P])$. By our assumption and by Theorem 15 of Section 3, the specialization ring $[[P] \xrightarrow{\mathfrak{o}} [\bar{P}]]$ is integrally

[11] Apply that proposition to $[A]$, $[\mathfrak{A}]_1$, $L \times S^m$ and $\mathfrak{L} \times \mathfrak{S}^m$, where S^m and $\mathfrak{S}^m$ denote the ambient spaces for V_α and $\bar{V}_\alpha$, respectively.

closed, so that by Proposition 5 of Section 1, it is a discrete valuation ring. Hence z has a uniquely determined specialization ζ over $[P] \xrightarrow{\mathfrak{o}} [\bar{P}]$; and ζ is a generalized quantity in $\kappa([\bar{P}])$. Denote by $\bar{\phi}$ the generalized function on $[\mathfrak{V}]$ defined by $\zeta = \bar{\phi}([\bar{P}])$ over κ. Thus we obtain a mapping $\phi \rightarrow \bar{\phi}$ from $\boldsymbol{F}$ to Φ; it is easy to see that this mapping does not depend on the choice of $[P]$ and $[\bar{P}]$. Therefore, we may call the field Φ the *field obtained from* $\boldsymbol{F}$ *by the reduction with respect to* $\mathfrak{p}$; of course, the field Φ depends upon the variety $[V]$ which is a "model" of $\boldsymbol{F}$.

THEOREM 20. *Let* $[V]$ *be a* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-variety defined over* k *and* $[\mathfrak{V}]$ *the abstract variety obtained from* $[V]$ *by the reduction with respect to* $\mathfrak{p}$. *Let* ϕ *be a function on* $[V]$ *defined over* k *such that* $\bar{\phi}$ *is a function on* $[\mathfrak{V}]$ *other than the constant* 0. *Then* $\rho((\phi)) = (\bar{\phi})$.

Proof. Let $[D]$ be the projective straight line defined over k and $[\mathfrak{D}]$ be the projective straight line defined over κ. We may consider $[\mathfrak{D}]$ as the abstract variety obtained from $[D]$ by reduction. Let Γ_ϕ be the graph of ϕ and $\Gamma_{\bar{\phi}}$ the graph of $\bar{\phi}$; then $\Gamma_{\bar{\phi}}$ is a component of $\bar{\Gamma}_\phi$. By Theorem 19, we have

$$\mathrm{pr}_{[\mathfrak{V}]}\{\rho(\Gamma_\phi)\} = \rho\{\mathrm{pr}_{[V]}(\Gamma_\phi)\} = \rho([V]) = [\mathfrak{V}].$$

By this equation we have $\rho(\Gamma_\phi) = \Gamma_{\bar{\phi}} + [\mathfrak{X}] \times [\mathfrak{D}]$, where $[\mathfrak{X}]$ is a $[\mathfrak{V}]$-divisor. Now by the definition of $(\phi)_0$, Theorem 17, Theorem 18, and Theorem 19, we have

$$\rho((\phi)_0) = \rho\{\mathrm{pr}_{[V]}(\Gamma_\phi \cdot [V]_0)\} = \mathrm{pr}_{[\mathfrak{V}]}\{(\Gamma_{\bar{\phi}} + [\mathfrak{X}] \times [\mathfrak{D}]) \cdot ([\mathfrak{V}] \times (0))\}$$
$$= \mathrm{pr}_{[\mathfrak{V}]}\{\Gamma_{\bar{\phi}} \cdot [\mathfrak{V}]_0 + [\mathfrak{X}] \times (0)\} = (\bar{\phi})_0 + [\mathfrak{X}].$$

Similarly, we have $\rho((\phi)_\infty) = (\bar{\phi})_\infty + [\mathfrak{X}]$; so we have $\rho((\phi)) = (\bar{\phi})$.

THEOREM 21. *Let* A^{n-1} *be a prime rational* S^n*-divisor over* k *and* (x) *a generic point of* A *over* k. *Let* $F(X) = 0$ *be an irreducible equation for* (x) *over* k *and suppose that* $F(X)$ *is a primitive polynomial in* $\mathfrak{o}[X]$. *Let* $\bar{F}(X) = \prod_\alpha \bar{G}_\alpha(X)^{\mu_\alpha}$ *be an expression of* $\bar{F}(X)$ *as a product of irreducible polynomials in* $\kappa[X]$. *Then, we have* $\rho(A) = \sum_\alpha \mu_\alpha \mathfrak{A}_\alpha$ *where, for each* α, $\mathfrak{A}_\alpha$ *is the prime rational* $\mathfrak{S}^n$*-divisor over* κ *which has a generic point* $(\xi^{(\alpha)})$ *over* κ *such that* $\bar{G}_\alpha(\xi^{(\alpha)}) = 0$.

Proof. Let $P = (t)$ and $\bar{P} = (\tau)$ be respectively a generic point of S^n over k and a generic point of $\mathfrak{S}^n$ over κ. Let ϕ be the function on S^n, defined over k by $F(t) = \phi(P)$. Then the function $\bar{\phi}$ on $\mathfrak{S}^n$ is defined

over κ by $\bar{F}(\tau) = \bar{\phi}(\bar{P})$. By our assumption on $F(X)$, the function $\bar{\phi}$ is not the constant 0; so that by Theorem 8 of [WF] Chapter VIII, Section 3 and by Theorem 20, we have $\rho(A) = \rho((\phi)) = (\bar{\phi})$. Let $\bar{\psi}_\alpha$ be the function on $\mathfrak{S}^n$ defined over κ by $\bar{G}_\alpha(\tau) = \bar{\psi}_\alpha(\bar{P})$, for each α. Then we have $\bar{\phi} = \prod_\alpha \bar{\psi}_\alpha^{\mu_\alpha}$; so we have by Theorem 6 and Theorem 8 of [WF] Chapter VIII, $(\bar{\phi}) = \sum_\alpha \mu_\alpha(\bar{\psi}_\alpha) = \sum_\alpha \mu_\alpha \mathfrak{A}_\alpha$. This proves our theorem.

5. Specialization-theory of cycles. When we consider the reduction of cycles with respect to $\mathfrak{p}$ as the specialization of cycles, our theory in Section 4 is concerned only with the specialization of the cycles which are rational over the basic field. In this section, we shall define a more general concept of the specialization of cycles on abstract varieties.

Let $[V]_1, \cdots, [V]_n$ be $\mathfrak{p}$-simple $\mathfrak{p}$-varieties defined over k and $[\mathfrak{V}]_1, \cdots, [\mathfrak{V}]_n$ be the abstract varieties obtained from $[V]_1, \cdots, [V]_n$ by the reduction with respect to $\mathfrak{p}$, respectively. Let $[X]_1, \cdots, [X]_n$ be respectively cycles on $[V]_1, \cdots, [V]_n$; and let $[\mathfrak{X}]_1, \cdots, [\mathfrak{X}]_n$ be respectively cycles on $[\mathfrak{V}]_1, \cdots, [\mathfrak{V}]_n$. We say that $([\mathfrak{X}]_1, \cdots, [\mathfrak{X}]_n)$ is a *specialization of* $([X]_1, \cdots, [X]_n)$ *over* $\mathfrak{o}$ if there exist an extension k' of k and a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ in k' such that $[X]_1, \cdots, [X]_n$ are all rational over k' and $[\mathfrak{X}]_1, \cdots, [\mathfrak{X}]_n$ are respectively the cycles obtained from $[X]_1, \cdots, [X]_n$ by the reduction with respect to $\mathfrak{o}'$. We shall denote by $([X]_1, \cdots, [X]_n) \xrightarrow{\mathfrak{o}} ([\mathfrak{X}]_1, \cdots, [\mathfrak{X}]_n)$.

PROPOSITION 26. *Let (x) be a set of n quantities in $\boldsymbol{K}$ and (ξ) a specialization of (x) over $\mathfrak{o}$. Then there exists a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ in $k(x)$ such that (ξ) is a specialization of (x) over $\mathfrak{o}'$.*

Proof. By Proposition 9 of Section 1, there exist an extension k_1 of k and a prolongation $\mathfrak{o}_1$ of $\mathfrak{o}$ in k_1 such that the residue field κ_1 of $\mathfrak{o}_1$ is $\kappa(\xi)$. Let (b) be a set of quantities in $\mathfrak{o}_1$ such that $(b) \xrightarrow{\mathfrak{o}_1} (\xi)$. We may assume that $k_1 = k(b)$. Let r be the dimension of (x) over k. Let the t_{ij} and the t_i for $1 \leqq i \leqq r$, $1 \leqq j \leqq n$ be $r(n+1)$ independent variables over k_1; and let the τ_{ij} and the τ_i for $1 \leqq i \leqq r$, $1 \leqq j \leqq n$ be $r(n+1)$ independent variables over κ_1. Put $k_2 = k_1(t_i, t_{ij})$ and $\mathfrak{o}_2 = [(t_i, t_{ij}) \xrightarrow{\mathfrak{o}_1} (\tau_i, \tau_{ij})]$; then $\mathfrak{o}_2$ is a prolongation of $\mathfrak{o}_1$ in k_2. Denote by L^{n-r} the linear variety

$$\left(\sum t_{ij}(X_j - b_j) - \pi t_i = 0 \quad (1 \leqq i \leqq r)\right)$$

in S^n where π is a prime element in $\mathfrak{o}$ and by $\mathfrak{L}^{n-r}$ the linear variety

$$\left(\sum \tau_{ij}(X_j - \xi_j) = 0 \quad (1 \leqq i \leqq r)\right)$$

in $\mathfrak{S}^n$; denote by A^r the prime rational cycle in S^n with the generic point (x) over k. Now we consider the reduction with respect to $\mathfrak{o}_2$. Then we have $\bar{L} = \mathfrak{L}$. The point (ξ) is contained in $\bar{A} \cap \mathfrak{L}$; moreover, since (τ) is a set of independent variables over κ_1, it can be easily proved that (ξ) is a component of $\bar{A} \cap \mathfrak{L}$. By Theorem 9 of Section 2, there exists a point (y) in $A \cap L$ such that (ξ) is a specialization of (y) over $\mathfrak{o}_2$. We extend the specialization ring $[(y) \xrightarrow{\mathfrak{o}_2} (\xi)]$ to a valuation ring $\mathfrak{o}_3$ in $k_3 = k_2(y)$; this valuation ring $\mathfrak{o}_3$ is also discrete as (y) is algebraic over k. Since L is a generic linear variety over k, we have $(x) \xleftrightarrow{k} (y)$. We extend this generic specialization to a generic specialization $(x, a, s) \xleftrightarrow{k} (y, b, t)$. Put $k_4 = k(x, a, s)$ and denote by $\mathfrak{o}_4$ the prolongation of $\mathfrak{o}$ in k_4 which corresponds to the prolongation $\mathfrak{o}_3$ in k_3 by the specialization $(x, a, s) \xleftrightarrow{k} (y, b, t)$. Put $\mathfrak{o}' = k(x) \cap \mathfrak{o}_4$; then $\mathfrak{o}'$ is a discrete valuation ring in $k(x)$ and it defines a prolongation of $\mathfrak{o}$ in $k(x)$ such that $(x) \xrightarrow{\mathfrak{o}} (\xi)$; so our proposition is proved.

By this proposition, our definition of the specialization of cycles does not conflict with the definition of the specialization of points. But it should be remarked that singular points or a pseudo-point are considered as the cycle 0.

PROPOSITION 27. *Let $[U]_1, \cdots, [U]_n$, $[V]_1, \cdots, [V]_m$ be $\mathfrak{p}$-simple $\mathfrak{p}$-varieties defined over k; and let $[X]_1, \cdots, [X]_n$, $[Y]_1, \cdots, [Y]_m$ be respectively cycles on $[U]_1, \cdots, [U]_n$, $[V]_1, \cdots, [V]_m$. Every specialization of $([X]_1, \cdots, [X]_n)$ over $\mathfrak{o}$ can be extended to a specialization of $([X]_1, \cdots, [X]_n, [Y]_1, \cdots, [Y]_m)$ over $\mathfrak{o}$.*

Proof. Let $([\mathfrak{X}]_1, \cdots, [\mathfrak{X}]_n)$ be a specialization of $([X]_1, \cdots, [X]_n)$ over $\mathfrak{o}$. Then, by our definition, there exist an extension k' of k and a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ in k' such that all the $[X]_i$ are rational over k' and that $\rho'([X]_i) = [\mathfrak{X}]_i$ for $1 \leqq i \leqq n$ where ρ' denotes the reduction-mapping with respect to $\mathfrak{o}'$. Let k'' be an extension of k' such that $[Y]_1, \cdots, [Y]_m$ are all rational over k'' and $\mathfrak{o}''$ a prolongation of $\mathfrak{o}'$ in k''. Put $[\mathfrak{Y}]_i = \rho''([Y]_i)$ for $1 \leqq i \leqq m$ where ρ'' denotes the reduction-mapping with respect to $\mathfrak{o}''$. Since $\rho''([X]_i) = \rho'([X]_i)$, we have

$$([X]_1, \cdots, [X]_n, [Y]_1, \cdots, [Y]_m) \xrightarrow{\mathfrak{o}} ([\mathfrak{X}]_1, \cdots, [\mathfrak{X}]_n, [\mathfrak{Y}]_1, \cdots, [\mathfrak{Y}]_m).$$

This proves our proposition.

Now we can easily prove that the specialization of cycles defined above preserves the operations on cycles.

THEOREM 22. *Let $[V]$ be a $\mathfrak{p}$-simple $\mathfrak{p}$-variety defined over k, $[X]$ and $[Y]$ two $[V]$-cycles of the same dimension and $([\mathfrak{X}], [\mathfrak{Y}])$ a specialization*

of $([X],[Y])$ *over* $\mathfrak{o}$. *Then* $[\mathfrak{X}]+[\mathfrak{Y}]$ *is a uniquely determined specialization of* $[X]+[Y]$ *over* $([X],[Y]) \xrightarrow{\mathfrak{o}} ([\mathfrak{X}],[\mathfrak{Y}])$.

THEOREM 23. *Let* $[V]$ *be a* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-variety defined over* k, $[X]^r$ *and* $[Y]^s$ *two positive* $[V]$*-cycles and* $([\mathfrak{X}],[\mathfrak{Y}])$ *a specialization of* $([X],[Y])$ *over* $\mathfrak{o}$. *If* $[X]\cdot[Y]$ *and* $[\mathfrak{X}]\cdot[\mathfrak{Y}]$ *are both defined, then* $[\mathfrak{X}]\cdot[\mathfrak{Y}]$ *is a uniquely determined specialization of* $[X]\cdot[Y]$ *over*

$$([X],[Y]) \xrightarrow{\mathfrak{o}} ([\mathfrak{X}],[\mathfrak{Y}]).$$

THEOREM 24. *Let* $[U]$ *and* $[V]$ *be two* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-varieties defined over* k, $[X]\times[Y]$ *a* $[U]\times[V]$*-cycle and* $([\mathfrak{X}],[\mathfrak{Y}])$ *a specialization of* $([X],[Y])$ *over* $\mathfrak{o}$. *Then,* $[\mathfrak{X}]\times[\mathfrak{Y}]$ *is a uniquely determined specialization of* $[X]\times[Y]$ *over* $([X],[Y]) \xrightarrow{\mathfrak{o}} ([\mathfrak{X}],[\mathfrak{Y}])$.

THEOREM 25. *Let* $[U]$ *and* $[V]$ *be two* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-varieties defined over* k *and denote by* $[\mathfrak{U}]$ *and* $[\mathfrak{V}]$ *the varieties obtained from* $[U]$ *and* $[V]$ *by the reduction with respect to* $\mathfrak{p}$, *respectively. Suppose that* $[V]$ *is* $\mathfrak{p}$*-complete and that* $[\mathfrak{V}]$ *has no multiple point. Let* $[X]$ *be a* $[U]\times[V]$*-cycle and* $[\mathfrak{X}]$ *a specialization of* $[X]$ *over* $\mathfrak{o}$. *Then* $\mathrm{pr}_{[\mathfrak{U}]}([\mathfrak{X}])$ *is a uniquely determined specialization of* $\mathrm{pr}_{[U]}([X])$ *over* $[X] \xrightarrow{\mathfrak{o}} [\mathfrak{X}]$.

We shall only prove Theorem 23 since the others are proved in the same way.

Proof of Theorem 23. Let $([\mathfrak{X}],[\mathfrak{Y}],[\mathfrak{Z}])$ be a specialization of $([X],[Y],[X]\cdot[Y])$ over $\mathfrak{o}$. By our definition, there exist an extension k' of k and a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ in k' such that $[X]$, $[Y]$ are rational over k' and $\rho'([X])=[\mathfrak{X}]$, $\rho'(Y)=[\mathfrak{Y}]$, $\rho'([X]\cdot[Y])=[\mathfrak{Z}]$, where ρ' denotes the reduction-mapping defined with respect to $\mathfrak{o}'$. Since $[\mathfrak{X}]\cdot[\mathfrak{Y}]$ is defined by our assumption, we have by Theorem 18 of Section 4, $\rho'([X]\cdot[Y]) = [\mathfrak{X}]\cdot[\mathfrak{Y}]$. This proves our theorem.

In case where $k=\mathfrak{o}$, we have a specialization-theory of cycles over a field. In this case, we have $[\mathfrak{U}]=[U]$ (or $[\mathfrak{U}]=[U]^\sigma$ where σ is an isomorphism of k) for an ambient variety $[U]$.

We have to prove that the specialization of cycles thus defined is transitive since this is not so obvious.

PROPOSITION 28. *Let* $[V]$ *be a* $\mathfrak{p}$*-simple* $\mathfrak{p}$*-variety defined over* k, $[X]'$ *a* V*-cycle and* $[\mathfrak{X}]$ *a specialization of* $[X]'$ *over* $\mathfrak{o}$.

i) *If* $[X]'$ *is a specialization of a* $[V]$*-cycle* $[X]$ *over* k, *then* $[\mathfrak{X}]$ *is a specialization of* $[X]$ *over* $\mathfrak{o}$.

ii) *Every specialization of* $[\mathfrak{X}]$ *over* κ *is also a specialization of* $[X]'$ *over* $\mathfrak{o}$.

Proof. Suppose that $[X] \xrightarrow{\mathfrak{k}} [X]' \xrightarrow{\mathfrak{o}} [\mathfrak{X}]$. Then, by our definition, there exist an extension k_1 of k and a discrete valuation ring $\mathfrak{o}_1$ in k_1 which contains k such that $[X]$ is rational over k_1 and $\rho_1([X]) = [X]'$ where ρ_1 is the reduction-mapping with respect to $\mathfrak{o}_1$; and there exist an extension k_2 of k and a prolongation $\mathfrak{o}_2$ of $\mathfrak{o}$ in k_2 such that $[X]'$ is rational over k_2 and $\rho_2([X]') = [\mathfrak{X}]$ where ρ_2 is the reduction-mapping with respect to $\mathfrak{o}_2$. By Proposition 9 of Section 1, there exist an extension k_3 of k_1 and a prolongation $\mathfrak{o}_3$ of $\mathfrak{o}_1$ in k_3 such that the residue field k_4 of $\mathfrak{o}_3$ contains k_2. Let $\mathfrak{o}_4$ be a prolongation of $\mathfrak{o}_2$ in k_4. Then we have $\rho_3([X]) = [X]'$, $\rho_4([X]') = [\mathfrak{X}]$ where ρ_3 and ρ_4 are the reduction-mappings with respect to $\mathfrak{o}_3$ and $\mathfrak{o}_4$, respectively. Let $\mathfrak{R}$ be the inverse image of $\mathfrak{o}_4$ by the natural homomorphism of $\mathfrak{o}_3$ onto k_4. Then $\mathfrak{R}$ is a (non-discrete) valuation ring with the quotient field k_3; we may consider the residue field of $\mathfrak{o}_4$ as the residue field of $\mathfrak{R}$. Denote by the $[A]_\lambda$ all the components of $[X]$. We may assume that the $[A]_\lambda$ are all defined over k_3. We fix our attention to one component $[A]_\lambda$ and one of its representative $A_{\lambda\alpha}$. Let S^n be the ambient space for $A_{\lambda\alpha}$, (x) a generic point of $A_{\lambda\alpha}$ over k_3 and the t_{ij} for $1 \leqq i \leqq r$, $1 \leqq j \leqq n$ rn independent variables over k where r is the dimension of $A_{\lambda\alpha}$. Put $y_i = \sum t_{ij}x_j$ for $1 \leqq i \leqq r$. Then we have an irreducible equation $F_{\lambda\alpha}(Y, T) = 0$ for (y_i, t_{ij}) over k_3. For each $[A]_\lambda$ and for each representative $A_{\lambda\alpha}$ of $[A]_\lambda$, we obtain such an equation. We may assume that the polynomials $F_{\lambda\alpha}$ are all primitive polynomials in $\mathfrak{R}[Y, T]$. Denote by c_ν all the coefficients of the $F_{\lambda\alpha}$. Let (γ) be the uniquely determined specialization of (c) over $\mathfrak{R}$. Then obviously we have $(c) \xrightarrow{\mathfrak{o}} (\gamma)$. By Proposition 26, there exists a prolongation $\mathfrak{o}'$ of $\mathfrak{o}$ in $k(c)$ such that $(c) \xrightarrow{\mathfrak{o}'} (\gamma)$. By Proposition 16 of Section 2 and by our definition of the reduction, we can easily prove that $[X]$ is rational over $k(c)$ and $\rho'([X]) = [\mathfrak{X}]$ where ρ' is the reduction-mapping with respect to $\mathfrak{o}'$. This proves the assertion i). The second assertion can be proved similarly.

6. Reduction with respect to infinitely many $\mathfrak{p}$. Let K be a field with a set of infinitely many discrete valuations $\{\omega_\lambda\}$. We denote by $\mathfrak{o}_\lambda$, $\mathfrak{p}_\lambda$ and κ_λ the valuation ring, the valuation ideal and the residue field of ω_λ, for every λ; denote by σ that set of valuations. In this section, we shall use these notations always in this sense. We assume that the set σ satisfies the following condition:

(I) *Every element of K other than zero is a $\mathfrak{p}_\lambda$-unit for almost all*[11] *the $\mathfrak{p}_\lambda$.*

[11] We shall use the term "almost all" in the sense of "all but a finite number of."

In the following we shall use the notations $\sigma_1, \sigma_2, \cdots$ for subsets of σ which contain almost all the $\mathfrak{p}_\lambda$.

Let V be a variety defined over K. We denote by $\bar{V}^{(\lambda)}$ the bunch obtained from V by the reduction with respect to $\mathfrak{p}_\lambda$, for every λ. Similarly, we use the notations $\rho_\lambda(X)$, $[\bar{V}]^{(\lambda)}$ and $\rho_\lambda([X])$ in the sense of the reduction with respect to $\mathfrak{p}_\lambda$.

PROPOSITION 29. *Let U be a variety in $S^n \times S^m$ defined over K with the projection V on S^n. If $[U:V]=1$, then the projection from U to V is regular along every component of $\bar{V}^{(\lambda)}$ for almost all the $\mathfrak{p}_\lambda$.*

Proof. Let (x,y) be a generic point of U over K; then we have expressions $y_j = F_j(x)/F(x)$ where $F(X)$ and $F_j(X)$ are polynomials in $K[X]$. By condition (I), $F(X)$ and the $F_j(X)$ are all contained in $\mathfrak{o}_\lambda[X]$ for almost all the $\mathfrak{p}_\lambda$. Let the t_{ij} $(1 \leqq i \leqq r, 1 \leqq j \leqq n)$ be rn independent variables over $K(x)$ and put $t_i = \sum t_{ij}x_j$ for $1 \leqq i \leqq r$. Let the $\tau_i^{(\lambda)}$ and the $\tau_{ij}^{(\lambda)}$ $(1 \leqq i \leqq r, 1 \leqq j \leqq n)$ be $r(n+1)$ independent variables over κ_λ, for every λ. Put $K' = K(t_i, t_{ij})$, $\mathfrak{o}_\lambda' = [(t_i, t_{ij}) \xrightarrow{\mathfrak{o}_\lambda} (\tau_i^{(\lambda)}, \tau_{ij}^{(\lambda)})]$; then, by Proposition 3 of Section 1, for every λ, $\mathfrak{o}_\lambda'$ is a discrete valuation ring with the quotient field K'. It is easy to see that the set σ' of all the valuations with the valuation rings $\mathfrak{o}_\lambda'$ also satisfies the condition (I). Since $K'(x)$ is finite algebraic over K', the set σ'' of all the valuations which are prolongations on $K'(x)$ of valuations in σ' also satisfies the condition (I); in particular, $F(x)$ is a unit for almost all valuations in σ''. Let $\mathfrak{V}_\lambda$ be a component of $\bar{V}^{(\lambda)}$ and $\mathfrak{L}_\lambda$ the linear variety $(\sum \tau_{ij}^{(\lambda)} X_j - \tau_i^{(\lambda)} = 0$ $(1 \leqq i \leqq r))$. Then we have a point $(\xi^{(\lambda)})$ in $\mathfrak{V}_\lambda \cap \mathfrak{L}_\lambda$. The valuation obtained from the specialization $(x) \xrightarrow{\mathfrak{o}_\lambda'} (\xi^{(\lambda)})$ is clearly in σ'', so that $\bar{F}^{(\lambda)}(\xi^{(\lambda)}) = 0$ only for a finite number of the $\mathfrak{p}_\lambda$, where $\bar{F}^{(\lambda)}$ is the class of F modulo $\mathfrak{p}_\lambda$. This proves our proposition.

LEMMA 3. *Let $F(X)$ be an absolutely irreducible polynomial in $K[X]$. Suppose that $F(X)$ is in $\mathfrak{o}_\lambda[X]$ for every λ, and denote by $\bar{F}^{(\lambda)}(X)$ the class of $F(X)$ modulo $\mathfrak{p}_\lambda$. Then $\bar{F}^{(\lambda)}(X)$ is absolutely irreducible for almost all the $\mathfrak{p}_\lambda$.*

Proof. We may assume that the degree of $F(X)$ is greater than 1 and that $\bar{F}^{(\lambda)}(X)$ has the same degree as $F(X)$ for every λ. Let the $M_\alpha^{(r)}$ be all the monomials in X whose degrees are less than or equal to r. Let d be the degree of F; and let r and s be a pair of positive integers such that $d = r + s$. Let $G_1(X) = \sum x_\alpha M_\alpha^{(r)}$ and $G_2(X) = \sum y_\beta M_\beta^{(s)}$ be two polynomials such that (x_α, y_β) is a set of independent variables over K, and put

$$H(X) = \sum z_\gamma M_\gamma^{(d)} = G_1(X)G_2(X).$$

We consider (x) and (y) as homogeneous coordinates of generic points of the projective spaces $[L]^{(r)}$ and $[L]^{(s)}$ over K, respectively. Also we consider (z) as homogeneous coordinates of a generic point of some projective variety $[V]$ over K. It is easy to see that (z) has actually a locus over K. By considering the "generic polynomials" over κ_λ, in the same way as above, we have points $(\xi^{(\lambda)})$, $(\eta^{(\lambda)})$ and $(\zeta^{(\lambda)})$ with loci $[\mathfrak{L}]_\lambda^{(r)}$, $[\mathfrak{L}]_\lambda^{(s)}$ and $[\mathfrak{B}]_\lambda$ over κ_λ, for every λ. It is easy to see that $(\xi^{(\lambda)}) \times (\eta^{(\lambda)}) \times (\zeta^{(\lambda)})$ is a specialization of $(x) \times (y) \times (z)$ over $\mathfrak{o}_\lambda$; so that $[\mathfrak{B}]_\lambda$ is contained in $[\bar{V}]_\lambda$. Now a polynomial $\sum c_\gamma M_\gamma^{(d)}$ in $K[X]$ of degree d has a factor of degree r in an extension of K if and only if (c) is a point of $[V]$; and a similar fact holds for a polynomial in $\kappa_\lambda[X]$ and the variety $[\mathfrak{B}]_\lambda$. In fact, the converse part is obvious; so we have only to prove the direct part. If (c) is a point in $[V]$, then (c) is a specialization of (z) over K. This specialization can be extended to a specialization $(a) \times (b) \times (c)$ of $(x) \times (y) \times (z)$ where $(a) \times (b)$ is a point in $[\mathfrak{L}]^{(r)} \times [\mathfrak{L}]^{(s)}$. By the equation $(\sum x_\alpha M_\alpha^{(r)})(\sum y_\beta M_\beta^{(s)}) = \sum z_\gamma M_\gamma^{(d)}$, we can easily verify (if necessary, we consider affine representatives) $(\sum a_\alpha M_\alpha^{(r)})(\sum b_\beta M_\beta^{(s)}) = h \sum c_\gamma M_\gamma^{(d)}$ where h is a quantity. Thus we have proved the above fact. Let $\mathfrak{a}$ be the ideal in $K[Z]$ determined by the set (z). Put $F(X) = \sum c_\gamma M_\gamma^{(d)}$; then by our assumption that F is absolutely irreducible, (c) is not a point in $[V]$; so that there exists a homogeneous polynomial $P(Z)$ in $\mathfrak{a}$ such that $P(c) \neq 0$. By our condition (I), the coefficients of $P(Z)$ and $P(c)$ are all $\mathfrak{p}_\lambda$-units for every $\mathfrak{p}_\lambda$ in some $\sigma_1 \subset \sigma$. Put $\bar{F}^{(\lambda)}(X) = \sum \bar{c}_\gamma^{(\lambda)} M_\gamma^{(d)}$ for every $\mathfrak{p}_\lambda$ in σ_1. If $\bar{F}^{(\lambda)}$ has a factor of degree r, then $(\bar{c}^{(\lambda)})$ is a specialization of $(\zeta^{(\lambda)})$ over κ_λ; so that it is a specialization of (z) over $\mathfrak{o}_\lambda$. Then from $P(z) = 0$ follows $\bar{P}^{(\lambda)}(\bar{c}^{(\lambda)}) = 0$; this is a contradiction if $\mathfrak{p}_\lambda \in \sigma_1$. Now if $\bar{F}^{(\lambda)}(X)$ is reducible, the degree r of one of the factors must satisfy $1 \leqq r \leqq [d/2]$; so our lemma is proved.

PROPOSITION 30. *Let V^r be a variety in S^{r+1} defined over K. Then V is $\mathfrak{p}_\lambda$-simple for almost all the $\mathfrak{p}_\lambda$.*

Proof. By Proposition 2 of [WF] Chapter IV, Section 1, V is defined by an absolutely irreducible equation $F(X) = 0$ with coefficients in K. By our condition (I), the coefficients of $F(X)$ are all $\mathfrak{p}_\lambda$-units for every $\mathfrak{p}_\lambda$ in some $\sigma_1 \subset \sigma$. Denote by $\bar{F}^{(\lambda)}(X)$ the class of $F(X)$ modulo $\mathfrak{p}_\lambda$ for every $\mathfrak{p}_\lambda$ in σ_1. Then by Lemma 3, $\bar{F}^{(\lambda)}$ is absolutely irreducible for every $\mathfrak{p}_\lambda$ in some $\sigma_2 \subset \sigma_1$. By Theorem 21 of Section 4, V is $\mathfrak{p}_\lambda$-simple for every $\mathfrak{p}_\lambda$ in σ_2; this proves our proposition.

THEOREM 26. *Let* $[V]$ *be an abstract variety defined over* K; *let* $[V]_\lambda$ *be a* $\mathfrak{p}_\lambda$*-variety with the underlying abstract variety* $[V]$, *for every* λ. *Suppose that* $[\bar{V}]_\lambda$ *is not empty for almost all the* $\mathfrak{p}_\lambda$. *Then* $[V]_\lambda$ *is* $\mathfrak{p}_\lambda$*-simple for almost all the* $\mathfrak{p}_\lambda$.[12]

Therefore, in this case, for almost all the $\mathfrak{p}_\lambda$, we can obtain the abstract variety $[\mathfrak{V}]_\lambda$ from $[V]_\lambda$ by the reduction with respect to $\mathfrak{p}_\lambda$; and $[\mathfrak{V}]_\lambda$ is defined over κ_λ.

Proof. We shall first prove our theorem in case where $[V]$ is a variety V^r in the affine space S^n. Let (x) be a generic point of V over K. Let the t_{ij} $(0 \leqq i \leqq r, 1 \leqq j \leqq n)$ be $(r+1)n$ independent variables over $K(x)$; and put $K' = K(t)$ and $y_i = \sum t_{ij}x_j$ for $0 \leqq i \leqq r$. Then by Proposition 16 of Section 2, we have $K'(x) = K'(y)$. Let W be the locus of (y) over K' in S^{r+1} and T the birational correspondence between V and W with the corresponding generic points (x) and (y) over K'. Let the $\tau_{ij}^{(\lambda)}$ $(0 \leqq i \leqq r, 1 \leqq j \leqq n)$ be $(r+1)n$ independent variables over κ_λ and put $\mathfrak{o}_\lambda' = [(t) \xrightarrow{\mathfrak{o}_\lambda} (\tau^{(\lambda)})]$. Then by Proposition 3 of Section 1, for every λ, $\mathfrak{o}_\lambda'$ is a discrete valuation ring with the quotient field K'. It is easy to see that the set σ' of all the valuations whose valuation rings are $\mathfrak{o}_\lambda'$ also satisfies (I). By Proposition 30, W is $\mathfrak{p}_\lambda'$-simple for every $\mathfrak{p}_\lambda'$ in some $\sigma_1' \subset \sigma'$. Denote by σ_1 the subset of σ corresponding to the subset σ_1' of σ'. Let $(\xi^{(\lambda)})$ be a generic point of a component $\mathfrak{V}_{\lambda 1}$ of $\bar{V}^{(\lambda)}$ over $\bar{\kappa}_\lambda(\tau^{(\lambda)})$, for every $\mathfrak{p}_\lambda$ in σ_1. Put $\eta_i^{(\lambda)} = \sum \tau_{ij}^{(\lambda)}\xi_j^{(\lambda)}$ for $0 \leqq i \leqq r$; then $(\xi^{(\lambda)}, \eta^{(\lambda)})$ is a specialization of (x, y) over $\mathfrak{o}_\lambda'$; and by Proposition 16 of Section 2, (x) is finite over $(y) \xrightarrow{\mathfrak{o}_\lambda'} (\eta^{(\lambda)})$. Let $\mathfrak{W}_\lambda$ be the variety obtained from W by the reduction with respect to $\mathfrak{p}_\lambda'$, for every $\mathfrak{p}_\lambda'$ in σ_1'. Since $\eta_i^{(\lambda)} = \sum \tau_{ij}^{(\lambda)}\xi_j^{(\lambda)}$, the dimension of $(\eta^{(\lambda)})$ over $\kappa_\lambda(\tau^{(\lambda)})$ is r; so that $(\eta^{(\lambda)})$ is a generic point of $\mathfrak{W}_\lambda$ over $\kappa_\lambda(\tau^{(\lambda)})$. By Theorem 15 of Section 3, $[(y) \xrightarrow{\mathfrak{o}_\lambda'} (\eta^{(\lambda)})]$ is integrally closed, so contains all the x_j since (x) is finite over $(y) \xrightarrow{\mathfrak{o}_\lambda'} (\eta^{(\lambda)})$. This shows that $(\xi^{(\lambda)})$ and $(\eta^{(\lambda)})$ are biregularly corresponding points by T. Then by Theorem 14 of Section 3, we have $\mu(V, \mathfrak{V}_{\lambda 1}) = \mu(W, \mathfrak{W}_\lambda) = 1$. Moreover if $\mathfrak{V}_{\lambda 2}$ is another component of $\bar{V}^{(\lambda)}$ then $\mathfrak{V}_{\lambda 2}$ also biregularly corresponds to $\mathfrak{W}_\lambda$, so it must coincide with $\mathfrak{V}_{\lambda 1}$. Thus our theorem is proved for an affine variety. Now we shall prove our theorem for an abstract variety $[V] = [V_\alpha; F_\alpha; T_{\beta\alpha}]$ on which a $\mathfrak{p}_\lambda$-variety $[V]_\lambda = [V_\alpha; F_\alpha; \mathfrak{F}_\alpha^{(\lambda)}; T_{\beta\alpha}]$ is

[12] This theorem may be considered as a generalization of a theorem of Bertini for pencils. (See O. Zariski, "Pencils on an algebraic variety and a new proof of a theorem of Bertini," *Transactions of the American Mathematical Society*, vol. 50 (1941), pp. 48-70.)

defined for every λ. As our theorem is proved for affine varieties, the varieties V_α and $T_{\beta\alpha}$ are all $\mathfrak{p}_\lambda$-simple for every $\mathfrak{p}_\lambda$ in some $\sigma_1 \subset \sigma$. Denote by $\mathfrak{V}_\alpha^{(\lambda)}$ the variety obtained from V_α by the reduction with respect to $\mathfrak{p}_\lambda$, for every α and every $\mathfrak{p}_\lambda$ in σ_1. By Proposition 29, for every α and β, $T_{\beta\alpha}$ is regular along $\mathfrak{V}_\alpha^{(\lambda)}$ and $\mathfrak{V}_\beta^{(\lambda)}$ for every $\mathfrak{p}_\lambda$ in some $\sigma_2 \subset \sigma_1$. Then by Theorem 13 of Section 3, there exists a component $\mathfrak{T}_{\beta\alpha}^{(\lambda)}$ of $\bar{T}_{\beta\alpha}^{(\lambda)}$ having the projection $\mathfrak{V}_\alpha^{(\lambda)}$. Since $T_{\beta\alpha}$ is $\mathfrak{p}_\lambda$-simple if $\mathfrak{p}_\lambda \varepsilon \sigma_1$, $\mathfrak{T}_{\beta\alpha}^{(\lambda)}$ is the only component of $\bar{T}_{\beta\alpha}^{(\lambda)}$ if $\mathfrak{p}_\lambda \varepsilon \sigma_2$; so that, by the same reason, the projection of $\mathfrak{T}_{\beta\alpha}^{(\lambda)}$ on $\bar{V}_\beta^{(\lambda)}$ is equal to $\mathfrak{V}_\beta^{(\lambda)}$. This shows that $\mathfrak{V}_\alpha^{(\lambda)}$ and $\mathfrak{V}_\beta^{(\lambda)}$ are biregularly corresponding varieties by $T_{\beta\alpha}$ for every $\mathfrak{p}_\lambda$ in σ_2. From this follows that, for every $\mathfrak{p}_\lambda$ in σ_2, $[\bar{V}]_\lambda$ has only one component $[\mathfrak{V}]_\lambda$. Furthermore, by our definition we have $\mu([V]_\lambda, [\mathfrak{V}]_\lambda) = \mu(V_\alpha, \mathfrak{V}_\alpha^{(\lambda)}) = 1$, if $[\mathfrak{V}]_\lambda$ has a representative in V_α. This proves our theorem.

UNIVERSITY OF TOKYO.

REFERENCES.

[1] M. Deuring, "Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers," *Mathematische Zeitschrift*, vol. 47 (1942), pp. 643-654.

[2] ———, "Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper," *Mathematische Annalen*, vol. 124 (1952), pp. 393-426.

[3] W. Krull, "Dimensionstheorie in Stellenringen," *Journal für die Reine und Angewandte Mathematik*, vol. 179 (1938), pp. 204-226.

[4] T. Matsusaka, "Specialization of cycles on a projective model," *Memoirs of the College of Science, University of Kyoto*, vol. 26 (1950), pp. 167-173.

[5] D. G. Northcott, "Specialization over a local domain," *Proceedings of the London Mathematical Society*, (III), vol. 1 (1951), pp. 129-137.

[6] P. Samuel, "La notion de multiplicité en algèbre et en géométrie algébrique," *Journal de Mathématique Pures et Appliquées*, (IX), vol. 30 (1951), pp. 159-274.

[7] A. Weil, *Foundations of algebraic geometry*, New York, 1946.

[8] ———, "Arithmetic on algebraic varieties," *Annals of Mathematics*, vol. 53 (1951), pp. 412-444.

COHERENCE INVARIANT MAPPINGS ON KRONECKER PRODUCTS.*

By Henry G. Jacob, Jr.

1. Introduction. The main objective in this paper is a generalization of a theorem on matrices proved by L. K. Hua [2]. By means of the concept of the rank of a matrix Hua has formulated the notion of coherence between pairs of matrices and defined the class of one-to-one coherence invariant mappings on the group $n \times m$ matrices. His theorem gives a complete characterization of this class for the case of matrices with entries in a field. The extension of Hua's results is suggested by the relationship between linear transformations of a finite dimensional space and matrices. Since in the finite dimensional setting the group of linear transformations is a special case of the broader notion of Kronecker products it appears natural to attempt to phrase a generalization in terms of Kronecker products of arbitrary dimensional spaces over division rings. This is accomplished by stating new definitions of rank and coherence for Kronecker products which reduce in the special case to the older forms. The generalized results are given in Theorem 5.1 of Section 5, and the last section is devoted to applications of this theorem.

2. The Kronecker product. As mentioned in the introduction, the system which serves as a foundation for this investigation is that of the Kronecker product of two vector spaces. We shall assume that $\mathfrak{X}$ and $\mathfrak{Y}$ are arbitrary left and right vector spaces respectively over the division ring Δ.

Definition 2.1. *$\mathfrak{X} \otimes \mathfrak{Y}$ is called the Kronecker product of the left vector space $\mathfrak{X}$ and the right vector space $\mathfrak{Y}$ if and only if,*

(i) *$\mathfrak{X} \otimes \mathfrak{Y}$ is a commutative group (composition denoted by $+$).*

(ii) *there exists a mapping $(x, y) \rightarrow x \otimes y$ of the product set $\mathfrak{X} \times \mathfrak{Y}$ into $\mathfrak{X} \otimes \mathfrak{Y}$ which, for all $x, x_1, x_2 \,\varepsilon\, \mathfrak{X}$, $y, y_1, y_2 \,\varepsilon\, \mathfrak{Y}$, $\alpha \,\varepsilon\, \Delta$ satisfies*

* Received September 30, 1953; revised November 6, 1954.

(a) $(x_1 + x_2) \otimes y = x_1 \otimes y + x_2 \otimes y$.

(b) $x \otimes (y_1 + y_2) = x \otimes y_1 + x \otimes y_2$.

(c) $x\alpha \otimes y = x \otimes \alpha y$.

(iii) *Every element of* $\mathfrak{X} \otimes \mathfrak{Y}$ *is of the form* $\sum x_i \otimes y_i$, $x_i \varepsilon \mathfrak{X}$, $y_i \varepsilon \mathfrak{Y}$.

(iv) (a) *If* $e_1, e_2, \cdots, e_m$ *is a finite set of linearly independent vectors in* $\mathfrak{X}$, *then the relation* $\sum^m{}_1 e_j \otimes y_j = 0$ *holds for* $y_j \varepsilon \mathfrak{Y}$ *only if all* y_j*'s* $= 0$.

(b) *If* $f_1, f_2, \cdots, f_n$ *is any finite set of linearly independent vectors in* $\mathfrak{Y}$, *then the relation* $\sum^n{}_1 x_j \otimes f_j = 0$ *holds for* $x_j \varepsilon \mathfrak{X}$ *only if all the* x_j*'s* $= 0$.

Properties (iv) (a) and (b) are called the independence conditions and it can be shown that any two groups which possess properties (i)-(iv) are isomorphic. A realization of this group is obtained by letting $\mathfrak{X}'$ be a left vector space dual to $\mathfrak{X}$ relative a bilinear form (x', x), $x' \varepsilon \mathfrak{X}'$, $x \varepsilon \mathfrak{X}$ [4]. For $x \varepsilon \mathfrak{X}$ and $y \varepsilon \mathfrak{Y}$ we define $x \otimes y$ to be the linear transformation $x' \rightarrow (x', x)y$ of $\mathfrak{X}'$ into $\mathfrak{Y}$. Then the set $\mathfrak{B} = [\sum x_i \otimes y_i \mid x_i \varepsilon \mathfrak{X}, y_i \varepsilon \mathfrak{Y}]$ is the Kronecker product of $\mathfrak{X}$ and $\mathfrak{Y}$.

3. Rank and coherence.

DEFINITION 3.1. *Let* $\mathfrak{X}$ *and* $\mathfrak{Y}$ *be right and left vector spaces respectively over the division ring* Δ. *Let* $\mathfrak{X} \otimes \mathfrak{Y}$ *denote the Kronecker product of these spaces. An element* $T = \sum x_i \otimes y_i$ *is of rank* n *if* n *is the minimum number of terms of the form* $x \otimes y$ *in which* T *can be expressed.*

DEFINITION 3.2. *Two elements* T *and* R *of* $\mathfrak{X} \otimes \mathfrak{Y}$ *are said to be coherent if* $T - R$ *has rank one.*

In the above realization of the Kronecker product as linear transformations, it is evident that rank as defined coincides with the more familiar notion for transformations. Now if we denote the rank of an element T by $r(T)$ we have as an obvious fact, that if T and R are elements of $\mathfrak{X} \otimes \mathfrak{Y}$, $r(T + R) \leqq r(T) + r(R)$.

DEFINITION 3.3. *If* $(x_1, x_2, \cdots, x_n)$ *is a set of vectors in* $\mathfrak{X}$, *the space generated by these will be denoted by* $[x_1, x_2, \cdots, x_n]$. *A similar notation will be used for subspaces generated by elements of* $\mathfrak{Y}$.

LEMMA 3.1. *An element* $T \varepsilon \mathfrak{X} \otimes \mathfrak{Y}$ *is of rank* n *if and only if* $T = \sum^n{}_1 x_i \otimes y_i$ *where the sets* $(x_1, x_2, \cdots, x_n)$ *and* $(y_1, y_2, \cdots, y_n)$ *are*

linearly independent. Furthermore, if T is of rank n and $T = \sum^n_1 x_i \otimes y_i = \sum^n_1 x_i^* \otimes y_i^*$, then

$$[x_1, x_2, \cdots, x_n] = [x_1^*, x_2^*, \cdots, x_n^*]$$

and

$$[y_1, y_2, \cdots, y_n] = [y_1^*, y_2^*, \cdots, y_n].$$

Proof. The necessity of the first statement is obvious. To prove the sufficiency assume that $T = \sum^n_1 x_i \otimes y_i$, where $(x_1, x_2, \cdots, x_n)$ and $(y_1, y_2, \cdots, y_n)$ each form linearly independents sets. Suppose that $r(T) < n$ and $T = -\sum^{n+k}_{n+1} x_j \otimes y_j$, $k < n$, where $(x_{n+1}, \cdots, x_{n+k})$ and $(y_{n+1}, \cdots, y_{n+k})$ are linearly independent sets. Then $\sum^{n+k}_1 x_i \otimes y_i = 0$. From the set $(y_1, y_2, \cdots, y_{n+k})$ select the maximal linearly independent subset which comprises the first n elements. We have then $(y_1, y_2, \cdots, y_n, y_{n+1}, \cdots, y_{n+s})$, $s \leqq k$ and $y_t = \sum^{n+s}_1 \gamma_j^t y_j$, $t = n+s+1, n+s+2, \cdots, n+k$, hence

$$\sum_{i=1}^{n+s} x_i \otimes y_i + \sum_{i=n+s+1}^{n+k} x_i \otimes (\sum_{j=1}^{n+s} \gamma_j^i y_j) = 0 \quad \text{or} \quad \sum_{j=1}^{n+s} [x_j + (\sum_{i=n+s+1}^{n+k} x_i \gamma_j^i)] \otimes y_j = 0.$$

By the assumed independence of $(y_1, y_2, \cdots, y_n, y_{n+1}, \cdots, y_{n+s})$, condition (iv)(a), mentioned earlier, implies that $x_j + (\sum^{n+k}_{n+s+1} x_i \gamma_j^i) = 0$ for $j = 1, 2, \cdots, n+s$. Since $k < n$, the independence of the set $(x_1, x_2, \cdots, x_n)$ is contradicted.

Assume next that T is of rank n and $T = \sum^n_1 x_i \otimes y_i = \sum^n_1 x_i^* \otimes y_i^*$. For simplicity write $x_k^* = -x_{n+k}$ and $y_k^* = y_{n+k}$, for $k = 1, 2, \cdots, n$. Then $T = \sum^n_1 x_i \otimes y_i = -\sum^{2n}_{n+1} x_j \otimes y_j$ which implies $\sum^{2n}_1 x_i \otimes y_i = 0$. Suppose that $[y_1, \cdots, y_n] \neq [y_1^*, y_2^*, \cdots, y_n^*]$ and $(y_1, y_2, \cdots, y_n, y_{n+1}, \cdots, y_{n+s})$ $0 < s \leqq n$ is a maximal linearly independent set selected from the y's. Following the same argument used in the preceding part of the proof we may show that the independence of the set $(x_1, x_2, \cdots, x_n)$ is contradicted.

The last lemma states that the sets $(x_1, x_2, \cdots, x_n)$ and $(y_1, y_2, \cdots, y_n)$ which appear in a minimal representation of an element T, where $r(T) = n$, will serve as basis for the spaces generated by any other two sets used in a minimal representation of T. The subspace $[x_1, x_2, \cdots, x_n]$ will be called *the right space associated with T* and the subspace $[y_1, y_2, \cdots, y_n]$ will be called *the left space associated with T*. A useful corollary of Lemma 3.2 is the following

COROLLARY 3.1. *$r(X - Y) = n$, for X and $Y \varepsilon \mathfrak{X} \otimes \mathfrak{Y}$, if and only if there exists a chain of $n-1$ elements $X_1, X_2, \cdots, X_{n-1}$ in $\mathfrak{X} \otimes \mathfrak{Y}$ such that*

$1 = r(X_1 - X) = r(Y - X_{n-1}) = r(X_i - X_{i-1})$, $1 < i < n$, *and there is no shorter chain with this property.*

We shall now begin a study of one-to-one mappings of one Kronecker product onto another which are coherence invariant, i. e. *a mapping is coherence invariant if whenever two elements are coherent their images are coherent.* We shall also require that the inverses of these mappings be coherence invariant. To establish the existence of such a mapping we shall describe two distinct types. Let $\mathfrak{X}_i$ and $\mathfrak{Y}_i$, $i = 1, 2$, be right and left vector spaces respectively over the division ring Δ_i. Suppose that P and Q are semi-linear transformations of $\mathfrak{X}_1$ into $\mathfrak{X}_2$ and $\mathfrak{Y}_1$ into $\mathfrak{Y}_2$ respectively with the same associated isomorphism of Δ_1 onto Δ_2. It is then true that the mapping $\sum x_i \otimes y_i \rightarrow \sum x_i P \otimes y_i Q$ of $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$ into $\mathfrak{X}_2 \otimes \mathfrak{Y}_2$, which we shall denote by $P \otimes Q$, is single-valued.* In the case where P and Q are one-to-one and onto $P \otimes Q$ is also one-to-one and coherence invariant, furthermore, the inverse $P^{-1} \otimes Q^{-1}$ possesses these properties. A second type of coherence invariant mapping different from the first is obtained in the following manner. Suppose that Δ_1' is an anti-isomorphic image of Δ_1, then the spaces $\mathfrak{X}_1$ and $\mathfrak{Y}_1$ may be regarded as left and right vector spaces respectively over Δ_1', and, as such, have associated with them the Kronecker product $\mathfrak{Y}_1 \square \mathfrak{X}_1$. It can be easily shown that the mapping $\sum x_i \otimes y_i \rightarrow \sum y_i \square x_i$ is a natural isomorphism of $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$ onto $\mathfrak{Y}_1 \square \mathfrak{X}_1$, which we shall denote by $\mathfrak{S}$. Now if Q and P are one-to-one semi-linear transformations of $\mathfrak{Y}_1$ onto $\mathfrak{X}_2$ and $\mathfrak{X}_1$ onto $\mathfrak{Y}_2$ with the same isomorphisms of Δ_1' onto Δ_2, the resultant mapping $\sum x_i \otimes y_i \rightarrow \sum y_i \square x_i \rightarrow \sum y_i Q \otimes x_i P$ is both one-to-one and coherence invariant of $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$ onto $\mathfrak{X}_2 \otimes \mathfrak{Y}_2$, and the same is true of the inverse.

We observe that the mappings of the two classes already described always carry the zero element of $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$ onto the zero of $\mathfrak{X}_2 \otimes \mathfrak{Y}_2$. Therefore, it should be remarked that a slightly more general coherence invariant mapping is obtained by the addition of a constant element in the image space. For example, consider the mapping $T \rightarrow T[P \otimes Q] + R$, where R is a fixed element of $\mathfrak{X}_2 \otimes \mathfrak{Y}_2$. Clearly this mapping has essentially the same properties as $P \otimes Q$.

At this point the question which naturally arises is whether or not the two classes described above comprise the totality of one-to-one coherence invariant mappings which have coherence invariant inverses and take zero

---

* This can be shown by an argument similar to that for the direct product of linear transformations [4].

onto zero. The answer, which is given in Theorem 5. 1, is in the affirmative when the dimensionalities of the vector spaces involved are greater than or equal to two and the division rings have more than two elements.

4. The fundamental theorem of affine geometry. Essential to the proof of the last statement of Section 3 is a well known theorem in affine geometry which we shall call the "fundamental theorem of affine geometry." The theorem will be stated for right vector spaces only, although similar results obtain for left vector spaces. The finite dimensional case over a field with three or more elements has been treated by Hua [2].

DEFINITION 4. 1. *If $\mathfrak{X}$ is a right vector space over a division ring Δ and $x_1, x_2 \in \mathfrak{X}$, the set of points $\mathfrak{L} = [x_1\alpha + x_2(1 - \alpha) \mid \alpha \in \Delta]$ is called the line through x_1 and x_2.*

THEOREM 4. 1. *Let $\mathfrak{X}_1$ and $\mathfrak{X}_2$ be right vector spaces over Δ_1 and Δ_2 respectively, with dimensionality greater than or equal to two. If Δ_1 contains more than two elements, then every one-to-one mapping P of $\mathfrak{X}_1$ onto $\mathfrak{X}_2$ which carries lines onto lines and zero onto zero is a semi-linear transformation.*

A comparison of Theorem 4. 1 with the "fundamental theorem of projective geometry" [1] will reveal that the minimum dimension in this case is one lower, however, an additional condition must be imposed on the division ring. The following example will show that this restriction cannot be removed. Let $\mathfrak{X}$ be a three dimensional vector space over Φ, the field of two elements. Denote by (x_1, x_2, x_3) a basis for $\mathfrak{X}$. It is clear that $\mathfrak{X}$ contains a total of eight elements which enumerated are $0, x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_2 + x_3$, and $x_1 + x_2 + x_3$. Consider the mapping P on $\mathfrak{X}$ which maps 0 onto $0, x_1 + x_2$ onto $x_1 + x_3$, $x_1 + x_3$ onto $x_1 + x_2$ and acts as the identity on the remaining elements. Since any line in $\mathfrak{X}$ contains just two elements (in particular a line determined by two points contains only these points) it is quickly seen that P is one-to-one on $\mathfrak{X}$ and carries lines onto lines. However, P is obviously not additive.

5. The main theorem. The notion of coherent sets, which is the fundamental tool in the analysis of coherence invariant mappings, will be introduced now.

DEFINITION 5. 1. (i) *A set $\mathfrak{S}$ contained in the Kronecker product $\mathfrak{X} \otimes \mathfrak{Y}$ is said to be a coherent set if every pair of elements of $\mathfrak{S}$ is coherent.*

(ii) *a maximal coherent set is a coherent set which is not properly contained in any other coherent set. Maximal coherent sets may frequently be referred to as simply maximal sets.*

(iii) *a maximal set containing the* 0 *element (hence, in addition, only elements of rank one) will be called a maximal set of rank one.*

DEFINITION 5.2. *We shall denote by $\mathfrak{Z}$ the group of mappings of $\mathfrak{X} \otimes \mathfrak{Y}$ of the form $T \to T_R = T + R$, R a fixed element of $\mathfrak{X} \otimes \mathfrak{Y}$. Two sets of $\mathfrak{X} \otimes \mathfrak{Y}$ are said to be equivalent under $\mathfrak{Z}$ if one is the image of the other under some element of $\mathfrak{Z}$.*

These mappings are analogous to translations in a vector space and are certainly one-to-one and coherence invariant. The same is true of the inverse, hence they leave invariant maximal sets and intersections of maximal sets.

NOTATION. (i) *If $x \varepsilon \mathfrak{X}$ and $y \varepsilon \mathfrak{Y}$ we shall denote by $x \otimes \mathfrak{Y}$ and $\mathfrak{X} \otimes y$ the sets $[x \otimes y \mid y \varepsilon \mathfrak{Y}]$ and $[x \otimes y \mid x \varepsilon \mathfrak{X}]$ respectively.*

(ii) *Since $T \to T^\delta$ denotes the natural isomorphism of $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$ onto $\mathfrak{Y}_1 \square \mathfrak{X}_1$, if $T = \sum x_i \otimes y_i$ then $T^\delta = \sum y_i \square x_i$. The resultant mapping $T \to T^\delta \to \sum y_i Q \otimes x_i P$, described earlier, will be denoted by $T \to (T^\delta)^\eta$.*

THEOREM 5.1. *Let $T \to T^\sigma$ be a one-to-one coherence invariant mapping of $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$ onto $\mathfrak{X}_2 \otimes \mathfrak{Y}_2$ which carries* 0 *onto* 0 *and possesses a coherence invariant inverse. Then either*

(1) *$T^\sigma = \sum x_i P \otimes y_i Q$, where P and Q are semi-linear transformations of $\mathfrak{X}_1$ onto $\mathfrak{X}_2$ and $\mathfrak{Y}_1$ onto $\mathfrak{Y}_2$ respectively with the same associated isomorphisms of Δ_1 onto Δ_2, or*

(2) *$T^\sigma = (T^\delta)^\eta = \sum y_i Q \otimes x_i P$, where P and Q are semi-linear transformations of $\mathfrak{X}_1$ onto $\mathfrak{Y}_2$ and $\mathfrak{Y}_1$ onto $\mathfrak{X}_2$ with the same associated isomorphisms of Δ'_1 onto Δ_2, regarding $\mathfrak{X}_1$ and $\mathfrak{Y}_1$ as left and right spaces over Δ'_1.*

We shall first establish the theorem for elements of rank one by examining the effect of σ on maximal sets of rank one. Two lemmas are required for this part of the proof.

LEMMA 5.1. *In the Kronecker product $\mathfrak{X} \otimes \mathfrak{Y}$ maximal sets of rank one are either of the form $x \otimes \mathfrak{Y}$ or $\mathfrak{X} \otimes y$ where x and y are non-zero elements of $\mathfrak{X}$ and $\mathfrak{Y}$ respectively.*

Proof. It follows from Lemma 3.1 that if Y is coherent to both 0 and

$X = x \otimes y \neq 0$, an element of rank one, then either $Y = x \otimes v$ or $Y = u \otimes y$. Thus if $\mathfrak{S}$ is a maximal set of rank one containing X, every element of $\mathfrak{S}$ is of one of these two types. Since $\mathfrak{S}$ is maximal, and dimension of $\mathfrak{X}$ and $\mathfrak{Y} \geqq 2$, it contains either a $u \otimes y$ where u and x are linearly independent or $x \otimes v$ where v and y are linearly independent. If both belong, then $\mathfrak{S}$ is no longer a coherent set.

LEMMA 5.2. *There are exactly two maximal sets containing a given pair of coherent elements. If the coherent elements $X = x_1 \otimes y$ and $X_2 = x_2 \otimes y$ are contained in the maximal sets $\mathfrak{S}_1$ and $\mathfrak{S}_2$, then*

$$\mathfrak{S}_1 \cap \mathfrak{S}_2 = [x_1\lambda + x_2(1 - \lambda) \otimes y \mid \lambda \varepsilon \Delta].$$

Proof. Let X_1 and X_2 be any pair of coherent elements. Choose from $\mathfrak{J}$ the mapping $T \to T - X_2$; then $X_1 \to x \otimes y$, an element of rank one, and $X_2 \to 0$. Now $x \otimes \mathfrak{Y}$ and $\mathfrak{X} \otimes y$ are the only maximal sets containing 0 and $x \otimes y$, hence the sets $\mathfrak{S}_1$ and $\mathfrak{S}_2$, equivalent to $x \otimes Y$ and $X \otimes y$ under this mapping, are the only maximal sets containing X_1 and X_2. To prove the second statement suppose $X_1 = x_1 \otimes y$ and $X_2 = x_2 \otimes y$ and apply the same mapping again. Then $\mathfrak{S}_1 \cap \mathfrak{S}_2$ is equivalent to the set $[(x_1 - x_2)\lambda \otimes y \mid \lambda \varepsilon \Delta]$.

Proof of the Theorem. From the assumptions about the mapping $T \to T^\sigma$, it is immediate that maximal sets of rank one and intersections of maximal sets are left invariant. As a consequence of this, if x_1 and w_1 are linearly independent elements of $\mathfrak{X}_1$, and $(x_1 \otimes \mathfrak{Y}_1)^\sigma$ and $(w_1 \otimes \mathfrak{Y}_1)^\sigma$ are images of $x_1 \otimes \mathfrak{Y}_1$ and $w_1 \otimes \mathfrak{Y}_1$ respectively, then either $(x_1 \otimes \mathfrak{Y}_1)^\sigma = x_2 \otimes \mathfrak{Y}_2$ and $(w_1 \otimes \mathfrak{Y}_1)^\sigma = w_2 \otimes \mathfrak{Y}_2$ where x_2, w_2 are linearly independent, or $(x_1 \otimes \mathfrak{Y}_1)^\sigma = \mathfrak{X}_2 \otimes y_2$ and $(x_1 \otimes \mathfrak{Y}_1) = \mathfrak{X}_2 \otimes z_2$ where y_2, z_2 are linearly independent in $\mathfrak{Y}_2$. Furthermore, if $(x_1 \otimes \mathfrak{Y}_1)^\sigma = x_2 \otimes \mathfrak{Y}_2$, then $(\mathfrak{X}_1 \otimes y_1)^\sigma = \mathfrak{X}_2 \otimes y_2$ must occur. Now it will be more convenient to restrict the remaining discussion to the case in which $(x_1 \otimes \mathfrak{Y}_1)^\sigma = x_2 \otimes \mathfrak{Y}_2$, however, it should be understood that the following arguments apply equally well to the other possible situation.

Since σ is one-to-one we may write $(x_1 \otimes y_1)^\sigma = x_2 \otimes y_1^\beta$, where $y_1 \to y_1^\beta$ is a one-to-one mapping of $\mathfrak{Y}_1$ onto $\mathfrak{Y}_2$. In fact, β possesses the additional property of carrying lines onto lines, which is seen by considering the line $[\lambda y_1 + (1 - \lambda) z_1 \mid \lambda \varepsilon \Delta_1]$ and recognizing, by Lemma 5.2, the set $[x_1 \otimes \lambda y_1 + (1 - \lambda) z_1 \mid \lambda \varepsilon \Delta_1]$ as the intersection of the maximal sets containing the coherent pair $x_1 \otimes y_1$ and $x_1 \otimes z_1$. The latter set, it follows, must map onto $[x_2 \otimes \gamma y_1^\beta + (1 - \gamma) z_1^\beta \mid \gamma \varepsilon \Delta_2]$ which is the intersection of the maximal sets containing the images $x_2 \otimes y_1^\beta$ and $x_2 \otimes z_1^\beta$. Thus by Theorem 4.1 we may assert that for each $x_1 \varepsilon \mathfrak{X}_1$ the mapping $y_1 \to y_1^\beta$ is a one-to-one

semi-linear transformation of $\mathfrak{Y}_1$ onto $\mathfrak{Y}_2$. Furthermore, from the coherence invariance of σ and the linearity of these induced mappings it can be seen that any two differ only by a scalar multiple. Similarly for each $y_1 \varepsilon \mathfrak{Y}_1$ there corresponds a one-to-one semi-linear transformation of $\mathfrak{X}_1$ onto $\mathfrak{X}_2$, and these also differ by scalars. Consequently, we may select a single mapping from each set, denote them by P_1 and Q_1, and write $(x_1 \otimes y_1)^\sigma = x_1P_1 \otimes \gamma(x_1, y_1)y_1Q_1$ for all elements of rank one, where $\gamma(x_1, y_1)$ appears to be dependent on x_1 and y_1. Actually $\gamma(x_1, y_1)$ is independent, and to show this we need only observe that the mappings $y_1 \to \gamma(x_1, y_1)y_1Q$, for x_1 fixed, and $x_1 \to x_1P_1\gamma(x_1, y_1)$, for y_1 fixed, are also semi-linear. Thus if P is the semi-linear transformation $x_1 \to x_1P_1\gamma(x_1, y_1)$ and $Q = Q_1$, we have $(x_1 \otimes y_1)^\sigma = x_1P \otimes y_1Q$. Clearly P and Q will have the same isomorphisms.

With the theorem established for elements of rank one we proceed with the final step. To simplfy this step we introduce the composite mapping $T \to T^\sigma[P^{-1} \otimes Q^{-1}]$ and denote it by π. π is one-to-one and coherence invariant on $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$, leaving the elements of rank one pointwise fixed. We shall prove that it is the identity on all of $\mathfrak{X}_1 \otimes \mathfrak{Y}_1$. Suppose that T is of rank n. By Lemma 3.1, if $T = \sum^n{}_1 x_i \otimes y_i$, the sets $(x_1, x_2, \cdots, x_u)$ and $(y_1, y_2, \cdots, y_u)$ are each linearly independent. It is immediate by Corollary 3.1 that $r(T) = r(T^\pi)$, hence we may write $T^\pi = \sum^n{}_1 x_j^* \otimes y_j^*$, where the x^*'s and y^*'s also form linearly independent sets. We observe next that $T - x_i \otimes y_i$, $1 \leqq i \leqq n$, is of rank $n-1$, therefore by Corollary 3.1 $T^\pi - (x_i \otimes y_i)^\pi = T^\pi - x_i \otimes y_i$ is of rank $n-1$. Thus $T^\pi = x_i \otimes y_i + \sum^{n-1}{}_1 x_{ik} \otimes y_{ik}$ for $1 \leqq i \leqq n$, and we have at once that $x_i \varepsilon [x_1^*, \cdots, x_n^*]$ and $y_i \varepsilon [y_1^*, y_2^*, \cdots, y_n^*]$. We may now write $T^\pi = \sum^n{}_1 x_j \otimes v_j$, where $(v_1, \cdots, v_n)$ is a linearly independent set in $\mathfrak{Y}_1$.

Consider the element $T - x_1 \otimes (y_1 + \lambda_2 y_2 + \cdots + \lambda_n y_n)$ which is of rank $n-1$ for all λ_j, $j = 2, 3, \cdots, n$. Then $T^\pi - x_1 \otimes (y_1 + \lambda_2 y_2 + \cdots + \lambda_n y_n)$ is of rank $n-1$, which implies $v_1 - y_1 = \sum^n{}_2 \xi_i v_i + \lambda_2 y_2 + \cdots + \lambda_n y_n$ for all λ_j. Let $\lambda_j = 0$, $j = 2, \cdots, n$, then $v_1 - y_1 = \sum^n{}_2 \xi_{1i}{}^{(1)} v_i$. By letting $\lambda_j = 0, j \neq k$, the last two equations give $y_k = \sum^n{}_2 \xi_{1i}{}^{(k)} v_i$, $k \neq 1$. Applying a similar argument to $T - x_j \otimes (\lambda_1 y_1 + \lambda_2 y_2 + \cdots + y_j + \cdots + \lambda_n y_n)$ we obtain

$$v_j - y_j = \sum_{i=1}^{n}{}' \xi_{ji}{}^{(j)} v_i \quad \text{and} \quad y_k = \sum_{i=1}^{n}{}' \xi_{ji}{}^{(k)} v_i, \qquad k \neq j,$$

where the primes refer to the exclusion of the summation index $i = j$. From these relations we have, for example, if $j = 2, 3, \cdots, n$,

$$v_1 = y_1 + \sum_{i=2}^{n} \xi_{1i}{}^{(1)} v_i = \sum_{i=1}^{n}{}' \xi_{ji}{}^{(1)} v_i + \sum_{i=2}^{n} \xi_{1i}{}^{(1)} v_i.$$

Since the v_i's are linearly independent, by letting j run from 2 to n we see $\xi_{1i}{}^{(1)} = 0$, $i = 2, 3, \cdots, n$, hence $v_1 = y_1$. By the same argument it can be shown that $v_i = y_i$, $i = 1, 2, \cdots, n$. Consequently, $T^\pi = T$ for all $T \varepsilon \mathfrak{X}_1 \otimes \mathfrak{Y}_1$ and $T^\sigma = T(P \otimes Q) = \sum^n{}_1 x_i P \otimes y_i Q$.

6. Applications. We turn our attention next to a situation in which we are given the dual pairs of vectors spaces $(\mathfrak{X}', \mathfrak{X})$ and $(\mathfrak{Y}', \mathfrak{Y})$ over the division ring Δ, with associated nondegenerate bilinear forms (x', x) $x' \varepsilon \mathfrak{X}'$, $x \varepsilon \mathfrak{X}$ and (y', y), $y' \varepsilon \mathfrak{Y}'$, $y \varepsilon \mathfrak{Y}$. We shall consider the additive group $\mathfrak{L}(\mathfrak{X}', \mathfrak{Y}')$ of linear transformations of $\mathfrak{X}'$ into $\mathfrak{Y}'$ which are continuous in the $\mathfrak{X}$-topology of $\mathfrak{X}'$ and $\mathfrak{Y}$-topology of $\mathfrak{Y}'$. It can be shown that these are just the linear transformations which possess adjoint mappings of $\mathfrak{Y}$ into $\mathfrak{X}$[4]. Moreover, the set $\mathfrak{F}(\mathfrak{X}', \mathfrak{Y}')$ of linear transformations of the form

$$x' \to (x', x_1) y_1' + (x', x_2) y_2' + \cdots + (x', x_n) y_n', \; x' \varepsilon \mathfrak{X}', x_1 \varepsilon \mathfrak{X}, y_i' \varepsilon \mathfrak{Y}', \quad 1 \leqq i \leqq n,$$

is a subset of $\mathfrak{L}(\mathfrak{X}', \mathfrak{Y}')$ which coincides with the set of all continuous linear transformations of finite rank. A transformation of this type will be denoted by $\sum x_i \otimes y_i'$. We have already seen that $\mathfrak{F}(\mathfrak{X}', \mathfrak{Y}')$ is the Kronecker product $\mathfrak{X} \otimes \mathfrak{Y}'$.

It should be mentioned that $\mathfrak{L}(\mathfrak{X}', \mathfrak{Y}')$ is a topological group in the finite topology, and $\mathfrak{F}(\mathfrak{X}', \mathfrak{Y}')$ is a dense subgroup of the full group of linear transformations of $\mathfrak{X}'$ into $\mathfrak{Y}'$. In addition $\mathfrak{L}(\mathfrak{X}', \mathfrak{Y}')$ may be considered as a left or right module over $\mathfrak{L}(\mathfrak{X}', \mathfrak{X}')$ or $\mathfrak{L}(\mathfrak{Y}', \mathfrak{Y}')$ respectively, where $\mathfrak{L}(\mathfrak{X}', \mathfrak{X}')$ is the ring of linear transformations in $\mathfrak{X}'$ with adjoints, and $\mathfrak{L}(\mathfrak{Y}', \mathfrak{Y}')$ is similarly defined for $\mathfrak{Y}'$. The subring $\mathfrak{F}(\mathfrak{X}', \mathfrak{X}')$ is a simple two sided ideal of $\mathfrak{L}(\mathfrak{X}', \mathfrak{X}')$ comprised of the union of minimal right ideals. Each minimal right ideal is generated by a idempotent transformation of rank one, hence the minimal ideals are composed of transformations of rank one and every transformation of rank one belongs to a minimal right ideal. Since $\mathfrak{L}(\mathfrak{X}', \mathfrak{Y}')$ is a left module over $\mathfrak{L}(\mathfrak{X}', \mathfrak{X}')$ we have the multiplication rule

$$(x_1 \times x_1')(x_2 \otimes y_2') = x_1 (x_1', x_2) \otimes y_2',$$

where $x_1 \times x_1' \varepsilon \mathfrak{X} \times \mathfrak{X}' = \mathfrak{F}(\mathfrak{X}', \mathfrak{X}')$ and $x_2 \otimes y_2' \varepsilon \mathfrak{X} \otimes \mathfrak{Y}' = \mathfrak{F}(\mathfrak{X}', \mathfrak{Y}')$.

Now consider the left module $\mathfrak{A}$ over $\mathfrak{R}$ such that $\mathfrak{F}(\mathfrak{X}', \mathfrak{Y}') \subseteqq \mathfrak{A} \subseteqq \mathfrak{L}(\mathfrak{X}', \mathfrak{Y}')$, $\mathfrak{F}(\mathfrak{X}', \mathfrak{X}') \subseteqq \mathfrak{R} \subseteqq \mathfrak{L}(\mathfrak{X}', \mathfrak{X}')$, and $\mathfrak{R}\mathfrak{A} \subseteqq \mathfrak{A}$. By the density property we have

LEMMA 6. 1. *If R, $S \in \mathfrak{R}$ and $RA = SA$ for all $A \in \mathfrak{A}$, then $R = S$. If $A, B \in \mathfrak{A}$ and $RA = RB$ for all $R \in \mathfrak{R}$, then $A = B$.*

Our purpose in this section is to investigate a one-to-one mapping σ of the module $\mathfrak{A}_1$ over $\mathfrak{R}_1$ onto the module $\mathfrak{A}_2$ over $\mathfrak{R}_2$, ($\mathfrak{A}_i$ and $\mathfrak{R}_i$, $i = 1, 2$, as described above) which satisfies the condition that $(R_1A_1)^\sigma = R_1{}^\gamma A_1{}^\sigma$ where $R_1 \to R_1{}^\gamma$ is a one-to-one mapping of $\mathfrak{R}_1$ onto $\mathfrak{R}_2$. In the process of characterizing this type of mapping we shall show that the associated mapping $R_1 \to R_1{}^\gamma$ is multiplicative, hence additive by a theorem of C. E. Rickart [5]. Moreover, an extension of Rickart's methods will be used to prove the additivity of σ. It will be assumed that the vector spaces and division rings involved satisfy the conditions imposed in Section 5.

LEMMA 6. 2. *Let $A_1 \to A_1{}^\sigma$ be a one-to-one mapping of $\mathfrak{A}_1$ onto $\mathfrak{A}_2$ such that $(R_1A_1)^\sigma = R_1{}^\gamma A_1{}^\sigma$ where $R_1 \to R_1{}^\gamma$ is a one-to-one mapping of $\mathfrak{R}_1$ onto $\mathfrak{R}_2$. Then the mapping σ is additive and γ is an isomorphism.*

Proof. Since $(R_1A_1)^\sigma = R_1{}^\gamma A_1{}^\sigma$ it follows that $(R_1S_1)^\gamma A_1{}^\sigma = R_1{}^\gamma S_1{}^\gamma A_1{}^\sigma$ for all $A_1 \in \mathfrak{A}_1$, hence by Lemma 6. 1 $(R_1S_1)^\gamma = R_1{}^\gamma S_1{}^\gamma$. Thus γ is multiplicative which implies γ is additive and, in fact, an isomorphism. Now since any element of rank one is contained in a minimal right ideal and minimal right ideals are mapped onto minimal right ideals under isomorphisms, we see that the additivity of γ implies the coherence invariance of γ. Furthermore, γ^{-1} is coherence invariant by the same argument, consequently $\mathfrak{F}(\mathfrak{X}_1', \mathfrak{Y}_1')$ is mapped onto $\mathfrak{F}(\mathfrak{X}_2', \mathfrak{Y}_2')$.

Next suppose A_1 and $B_1 \in \mathfrak{F}(\mathfrak{X}_1', \mathfrak{Y}_1')$ and have disjoint right spaces associated with minimal representations; i. e., $A_1 = \sum^n{}_1\, x_i \otimes y_i'$ and $B_1 = \sum^m{}_1\, u_i \otimes v_i'$, where $(x_1, x_2, \cdots, x_n, u_1, \cdots, u_m)$ form a linearly independent set. Let $x_{n+k} = u_k$, $k = 1, 2, \cdots, m$, then by the assumption that $(\mathfrak{X}_1', \mathfrak{X}_1)$ comprise a dual pair of vector spaces there exist $x_1', x_2', \cdots, x_{n+m}'$, $x_i' \in \mathfrak{X}_1'$ such that $(x_i', x_j) = \delta_{ij}$. If $R_1 = \sum^n{}_1\, x_i \times x_i'$ and $S_1 = \sum^{m+n}{}_{n+1}\, x_j \times x_j'$, it is apparent that $R_1A_1 = A_1$, $R_1B_1 = 0$, $S_1B_1 = B_1$ and $S_1A_1 = 0$. Thus by the additivity of γ and the equation $(R_1 + S_1)(A_1 + B_1) = A_1 + B_1$, we have $(A_1 + B_1)^\sigma = A_1{}^\sigma + B_1{}^\sigma$. Furthermore, an induction argument may be used to show that $A_1{}^\sigma = \sum^n{}_1 (x_i \otimes y_i)^\sigma$, whenever the x_i's are linearly independent. Consider next the case in which $A_1 = x_1 \otimes y'$ and $B_1 = x_1 \otimes v'$. Since $\mathfrak{X}_1$ has dimension greater than or equal to two there exists $x_1{}^* \in \mathfrak{X}_1$ such that x_1 and $x_1{}^*$ are linearly independent. If $C_1 = x_1{}^* \otimes y$, then $A_1 + B_1 = x_1 \otimes (y' + v')$ and $A_1 + C_1 = (x_1 + x_1{}^*) \otimes y$, thus from the preceding remarks it follows that

$$((A_1 + B_1) + C_1)^\sigma = (A_1 + B_1)^\sigma + C_1^\sigma$$

$$((A_1 + C_1) + B_1)^\sigma = (A_1 + C_1)^\sigma + B_1^\sigma = A_1^\sigma + C_1^\sigma + B_1^\sigma.$$

Therefore $(A_1 + B_1)^\sigma = A_1^\sigma + B_1^\sigma$.

We are now prepared to deal with the case in which A_1 and B_1 are arbitrary elements of $\mathfrak{F}(\mathfrak{X}_1', \mathfrak{Y}_1')$. Assume that the set $(x_1, x_2, \cdots, x_{n+1} \cdots x_{n+m})$ is not linearly independent and select from it the maximal linearly independent set $(x_1, x_2, \cdots, x_n, x_{n+1}, \cdots, x_{n+t})$, where $0 \leqq t < m$. Then we may write $B_1 = \sum^n{}_1\, x_i \otimes w_i' + \sum^{n+t}{}_{n+1}\, x_j \otimes w_j'$ and

$$A_1 + B_1 = \textstyle\sum^n{}_1\, x_i \otimes (y_i' + w_i') + \sum^{n+t}{}_{n+1}\, x_j \otimes w_j'.$$

From these equations it is easily shown that σ is additive on $\mathfrak{F}(\mathfrak{X}_1', \mathfrak{Y}_1')$.

Finally, to show σ is additive on all of $\mathfrak{A}_1$, it is sufficient, in view of Lemma 6.1, to observe that for A_1 and B_1 in $\mathfrak{A}_1$, $R_1^\gamma(A_1^\sigma + B_1^\sigma) = R_1^\gamma(A_1 + B_1)^\sigma$ for all $R_1 \in \mathfrak{F}(\mathfrak{X}_1', \mathfrak{X}_1')$.

THEOREM 6.1. *Let* $A_1 \to A_1^\sigma$ *be as defined in Lemma* 6.1. *Then* $A_1^\sigma = T_1{}^*A_1Q_1$ *and* $R_1^\gamma = T_1{}^*R_1T_1{}^{*-1}$, *where* $T_1{}^*$ *and* Q_1 *are one-to-one semi-linear transformations of* $\mathfrak{X}_2'$ *onto* $\mathfrak{X}_1'$ *and* $\mathfrak{Y}_1'$ onto $\mathfrak{Y}_2'$ *respectively.*

Proof. In the proof of Lemma 6.2 we showed γ is coherence invariant. We must also show the same is true of σ. Suppose $L_1 = x_1 \otimes y_1'$. There exists $F_1 = x_1 \times x_1'$ such that $(x_1, x_1') = 1$, hence $F_1L_1 = L_1$ and $(L_1)^\sigma = F_1^\gamma L_1^\sigma$. But F_1 is of rank one, consequently $F_1^\gamma L_1^\sigma$ is of rank one. Since σ is also additive it must be coherent invariant. σ^{-1} is coherence invariant for the same reasons.

We may now conclude by Theorem 5.1 that for all

$$F_1 = \textstyle\sum x_i \times x_i' \in \mathfrak{F}(\mathfrak{X}_1', \mathfrak{X}_1')$$

either (1) $F_1^\gamma = \sum x_iT_1 \times x_i'T_1'$ or (2) $F_1^\gamma = \sum x_i'T_1' \times x_iT_1$, and for all $L_1 \in \mathfrak{F}(\mathfrak{X}_1', \mathfrak{Y}_1')$ either (3) $L_1^\sigma = \sum x_jP \otimes y_j'Q$ or (4) $L_1^\sigma = \sum y_j'Q \otimes x_jP$. To start with we shall assume that forms (1) and (3) hold simultaneously. Later we show that this is the only possible combination.

Suppose that $F_1 = x_1 \times x_1'$ and $L_1 = x_1 \otimes y_1'$. Then

$$F_1L_1 = x_1(x_1', x_1) \otimes y_1', \quad \text{hence} \quad (F_1L_1)^\sigma = (x_1(x_1', x_1))P \otimes y_1'Q.$$

By assumption

$$\begin{aligned}(F_1L_1)^\sigma = F_1^\gamma L_1^\sigma &= (x_1T_1 \times x_1'T_1')(x_1P \otimes y_1'Q)\\ &= x_1T_1(x_1'T_1', x_1P) \otimes y_1'Q,\end{aligned}$$

and thus $x_1P(x_1', x_1)^\tau = x_1T_1(x_1'T_1', x_1P)$, where τ is the isomorphism associated with P. Since P and T are one-to-one and differ for each $x_1 \varepsilon \mathfrak{X}_1$ by a scalar multiple, we have that $x_1P = x_1T_1\alpha$, α fixed in Δ_2. Moreover, if λ is the isomorphism associated with T_1, then $\gamma^\lambda = \alpha\gamma^\tau\alpha^{-1}$, $\gamma \varepsilon \Delta_1$. Thus $\alpha(x_1', x_1)^\tau = (x_1'T_1', x_1T_1)\alpha$, from which follows $(x_1', x_1)^\lambda = (x_1'T_1', x_1T_1)$. Since T_1 and T_1' have inverses, the last relation states

$$(x_2', x_1T_1)^{\lambda^{-1}} = (x_2'T_1'^{-1}, x_2).$$

In other words, T_1 has as adjoint $T_1^* = T_1'^{-1}$, consequently if $y_1Q_1 = \alpha y_1Q$, then $(F_1L_1)^\sigma = T_1^*(F_1L_1)Q_1$, $F_1^\gamma = T_1^*F_1T_1^{*-1}$, and $L_1^\sigma = T_1^*L_1Q_1$ for all L_1 and F_1. Again Lemma 6.1 can be used to prove that σ takes this form for all $A_1 \varepsilon \mathfrak{A}_1$. Moreover, since it is evident that γ is, in fact, a special case of σ when we identify $\mathfrak{A}_1$ with $\mathfrak{R}_1$, it is also clear that γ has the same form on all of R_1.

Finally we may dispose of the other combinations by considering only the combination (1) and (4) and remarking that a similar argument can be used for the others. Suppose then that F_1 and L_1 are defined as before and $(F_1L_1)^\sigma = y_1'Q \otimes (x_1(x_1', x_1))P$ and $F_1^\gamma L_1^\sigma = x_1T_1(x_1'T_1', y_1'Q) \otimes x_1P$. Therefore, $y_1'Q(x_1', x_1)^\tau = x_1T_1(x_1'T_1', y_1'Q)$ for all $y_1' \varepsilon \mathfrak{Y}_1'$, $x_1 \varepsilon \mathfrak{X}_1$, $x_1' \varepsilon \mathfrak{X}_1'$. Clearly if y_1 is fixed and x_1 allowed to vary, this situation is impossible. This completes the proof.

By means of Theorem 6.1 we may readily obtain the isomorphism theorem for primitive rings with minimal ideals [3]. This result can be stated as follows.

THEOREM 6.2. *Let $(\mathfrak{X}_1', \mathfrak{X}_1)$ and $(\mathfrak{X}_2', \mathfrak{X}_2)$ be dual pairs of vector spaces over Δ_1 and Δ_2 respectively. Let $\mathfrak{A}_i$, $i = 1, 2$, be primitice rings with minimal ideals such that $\mathfrak{F}(\mathfrak{X}_i', \mathfrak{X}_i) \subseteqq \mathfrak{A}_i \subseteqq \mathfrak{L}(\mathfrak{X}_i', \mathfrak{X}_i')$. If $A_1 \rightarrow A_1^\sigma$ is an isomorphism of $\mathfrak{A}_1$ onto $\mathfrak{A}_2$, then $A_1^\sigma = T_1^*A_1T_1^{*-1}$, where T_1^* is a one-to-one semi-linear transformation of $\mathfrak{X}_2'$ onto $\mathfrak{X}_1'$.*

LOUISIANA STATE UNIVERSITY.

BIBLIOGRAPHY.

[1] R. Baer, *Linear algebra and projective geometry*, New York, 1952.

[2] L. K. Hua, "A theorem on matrices and its application to Grassmann space," *Science Reports of the National Tsing Hua University*, Ser. A, vol. 5 (1948), pp. 150-181.

[3] N. Jacobson, "On the theory of primitive rings," *Annals of Mathematics*, vol. 48 (1947), pp. 8-21.

[4] ———, *Lectures in abstract alegbra*, vol. I, New York (1951), vol. II, New York (1953).

[5] C. E. Rickart, "One-to-one mappings of rings and lattices," *Bulletin of the American Mathematical Society*, vol. 54 (1948), pp. 758-764.

A CHARACTERIZATION OF A CLASS OF RINGS.*

By R. L. San Soucie.

1. Introduction. Skornyakov [4] has shown that *a right alternative division ring of characteristic not two is alternative,* while the author has proved [2] that *a right alternative division ring of characteristic two is alternative if and only if it satisfies the identity*

$$(1.1) \qquad w(xy \cdot x) = (wx \cdot y)x.$$

Moreover, R. H. Bruck has actually constructed examples of right alternative division rings which are not alternative. This construction is detailed in an appendix to [2], but may be summarized as follows.

Let F be any field of characteristic two for which there exists an automorphism α of order 2 and an element f_0 in F such that $f_0\alpha = f_0$ and f_0 not a square in F. Let θ be the additive endomorphism of F defined by $f\theta = f\alpha + f_0 f$, all f in F. Then if R is the set of all couples (f, g), with f, g in F, if equality and addition in R are defined componentwise and multiplication is defined by

$$(1.2) \qquad (f, g)(h, k) = (fh + g \cdot k\theta, fk + gh),$$

R is a right alternative division ring of characteristic two which is not alternative. A field F which suffices is $F = B(t)$, where B is any field of characteristic two and t is transcendental over B. Then, for any $f(t)$ in $B(t)$, α defined by $f(t)\alpha = f(t+1)$ and $f_0 = t^2 + t$ can be used to construct the required endomorphism θ. (The elaborate choice of θ is explained in [2], and does not concern us here.)

In view of the above, we make the following definition. If B is a not alternative, right alternative division ring of characteristic two, if B is two-dimensional over some field F (so that B can be written as the set of all couples (f, g) with f, g in F) and if multiplication in B is given by (1.2), where θ is some additive endomorphism of F, not necessarily, however, the particular kind mentioned above, then we shall call B a *Bruck ring.* Since the rings whose construction was outlined above fall into this class, the class is not empty. Moreover, Bruck rings have the following surprising properties:

* Received November 8, 1954.

1. The identity $(w, x, yz) + (w, y, xz) = (w, x, z)y + (w, y, z)x$ holds in any Bruck ring B, although it can be obtained by linearization from (1.1), which cannot hold in B.
2. The identity $(wx, y, z) = w(x, y, z) + (w, y, z)x + (w, x, (y, z))$ is satisfied by any choice of w, x, y, z in any B, and this identity played an important role in proving that other right alternative rings were alternative. (See [1], [2], [3], and [4].)
3. The left nucleus K, of any B, commutes with B, and squares and commutators are all in K.

In view of these properties, we concern ourselves in this paper with the following problem: what characterizes the Bruck rings in the class of all not alternative, right alternative division rings of characteristic two? The answer turns out to be simple. Property 2 and a part of property 3 (above) together provide necessary and sufficient conditions for a not alternative right alternative division ring to be a Bruck ring.

All of our results appear to be new, for (to our knowledge) there is no literature concerning right alternative rings that does not either prove or assume (1.1). But some of our methods are similar to those used in [2]. We intentionally omit the verification of properties 1, 2, and 3 for Bruck rings. Nothing is involved except tedious computation using (1.2) and this does not seem worth recording here.

2. Preliminary results. Throughout the paper, R will always denote a right alternative ring of characteristic two.

LEMMA 1. *The following identities hold in R:*

$$(wx, y, z) + (w, xy, z) + (w, x, yz) = w(x, y, z) + (w, x, y)z \tag{2.1}$$

$$(xy, z) = x(y, z) + (x, z)y + (z, x, y) \tag{2.2}$$

$$((x, y), z) + ((x, z), y) + ((y, z), x) = 0. \tag{2.3}$$

These identities are well-known. (See [5], page 125.)

Definition 1. R will be said to have *property A* if R is not alternative and if

$$(wx, y, z) = w(x, y, z) + (w, y, z)x + (w, x, (y, z)) \tag{2.4}$$

holds identically in R.

We now derive some consequences of the definition.

LEMMA 2. *Let R have property A. Then the following identities hold in R:*

$$(2.5) \qquad (w, x, yz) + (w, y, xz) = (w, x, z)y + (w, y, z)x$$

$$(2.6) \qquad (w, x, (y, z)) + (w, y, (x, z)) + (w, z, (x, y)) = 0$$

$$(2.7) \qquad (w, x^2, y) = (w, x, y)x + (w, x, yx)$$

$$(2.8) \qquad (w, y, x) \cdot yx + (w, y, x)x \cdot y = (w, y, yx^2) + (w, y, x^2)y.$$

Proof. (2.5) is obtained by direct substitution of (2.4) into (2.1) and collecting terms. (2.6) then follows from (2.5) by expansion of the left member of (2.6). (2.7) then comes from (2.5) via the substitution $x \to y$, $y \to x$, $z \to x$. Now $(w, y, yx^2) = (w, y, x) \cdot yx + (w, yx, x)y$ using (2.5) and also $(w, yx, x)y = (w, y, x^2)y + (w, y, x)x \cdot y$ using (2.7). This proves (2.8) and the lemma.

The following definition is standard.

Definition 2. Let

$$K = [k \,\varepsilon\, R \mid (k, R, R) = 0], \text{ let } M = [m \,\varepsilon\, R \mid (R, R, m) = 0],$$

and let $C = [c \,\varepsilon\, M \mid (c, R) = 0]$. Then we call K the *left nucleus* of R, M the *right nucleus* of R, and C the *centre* of R. Observe that C is in K by (2.2).

LEMMA 3. *Let R have property A and have no proper divisors of zero. Then $M = C$.*

Proof. Clearly we need only prove $M \subset C$. Select $x \,\varepsilon\, R$, $x \not\varepsilon\, M$. Then, for any $m \,\varepsilon\, M$, $(R, x, m) = 0$ and $(x, m) \,\varepsilon\, M$, using (2.4). But also $(R, x, xm) = 0$ so that $(x, xm) \,\varepsilon\, M$. However, $(xm, x) = x(m, x)$ and the latter implies $x \,\varepsilon\, M$, a contradiction, unless $(m, x) = 0$. Hence $0 = (xm, m') = x(m, m')$ and thus $(M, R) = 0$. This proves the lemma.

Definition 3. If R is a ring with property A and if R is such that all commutators are in the left nucleus, then we shall say that R also has the *commutator property.* For convenience, we shall write that R has *property ACP.*

LEMMA 4. *Let R have property ACP and no proper divisors of zero. Then* (i) $(K, K) = 0$, (ii) $(x^2, R) = 0$, (iii) $x^2 \,\varepsilon\, K$, (iv) $((x, y), R) = 0$, (v) $(R, x^2, (y, z)) = 0$, (vi) $(R, x^2, y^2) \subset K$.

Proof. Select $x \,\varepsilon\, R$, $x \not\varepsilon\, K$, and $k, k' \,\varepsilon\, K$. Then

$$(xk, k') = x(k, k') + (x, k')k$$

and thus $x(k, k') \in K$. But the latter implies that $x \in K$, a contradiction, unless $(k, k') = 0$. This proves (i). Since

$$(xy, x) = x(y, x) + (x, x, y), \tag{2.9}$$

we have

$$((x, x, y), x, y) = (x(y, x), x, y) = (x, x, y)(x, y)$$

and also

$$((x, x, y), x, y) = ((y, x)x, x, y) = (x, y)(x, x, y)$$

so that

$$((x, y), (x, x, y)) = 0. \tag{2.10}$$

We conclude from (2.10) and (2.9) that $0 = (x(x, y), (x, y)) = (x, (x, y))(x, y)$ and this implies that $(x, (x, y)) = 0$. Hence $(x^2, y) = x(x, y) + (x, y)x = 0$ and $(x^2, R) = 0$. (ii) and (2.2) prove (iii), while (iv) follows from (ii) by replacing x by $x + y$. Replacing x by x^2 in (2.6) then yields (v), and (vi) comes from the observation that $(x^2y^2, u) = (u, x^2, y^2)$.

Henceforth we shall assume that R is a division ring with property *ACP*. This added assumption enables us to prove a lemma which is crucial to our theory. It is perhaps worth noting that the identity of the lemma has heretofore been proved using (1.1).[1]

LEMMA 5. *The following identity holds in R:*

$$((w, x, y), x, y) = (w, x, y)(x, y). \tag{2.11}$$

Proof. We begin by observing that

$$(w, y, yx^2) = (w, y, x^2y) = (w, x^2, y^2) + (w, x^2, y)y.$$

Hence (2.8) becomes

$$(w, y, x) \cdot yx + (w, y, x)x \cdot y = (w, x^2, y^2). \tag{2.12}$$

Then

$$\begin{aligned}((w, x, y), x, y) &= (w, x, y) \cdot xy + (w, x, y)x \cdot y \\ &= (w, x, y) \cdot xy + (w, x, y) \cdot yx + (w, x^2, y^2),\end{aligned}$$

using (2.12), so that

$$((w, x, y), x, y) = (w, x, y)(x, y) + (w, x^2, y^2). \tag{2.13}$$

[1] But we should point out that previous proofs did not need the division ring hypothesis.

We now complete the proof by showing that $(w, x^2, y^2) = 0$, and begin by noting that (2.9) implies

$$((x, x, y), x, y) = (x, x, y)(x, y), \tag{2.14}$$

while (2.13) yields

$$((x, x, y), x, y) = (x, x, y)(x, y) + (x, x^2, y^2). \tag{2.15}$$

Therefore (2.14) and (2.15) together yield

$$(x, x^2, y^2) = 0. \tag{2.16}$$

The substitution $x \to x + y$, $y \to z$ in (2.16) yields the linearized identity

$$(y, x^2, z^2) = (x, y^2, z^2) \tag{2.17}$$

and setting $y = k$ in (2.17) gives

$$(x, k^2, z^2) = 0. \tag{2.18}$$

Now consider $q = (w, x^2, y^2)$. If either x or y is in K, $q = 0$ by (2.18). Hence we can assume without loss of generality that $x \not\in K$ and then we define z by $xz = w$, for the particular x and w chosen in the associator q. This gives

$$q = (xz, x^2, y^2) = x(z, x^2, y^2). \tag{2.19}$$

But $q \varepsilon K$ by Lemma 4(vi), and (z, x^2, y^2) is in K also. Hence (2.19) implies that x is in K, a contradiction, unless $(z, x^2, y^2) = 0$. But then $q = 0$, (2.13) becomes (2.11) and the lemma is proved.

3. The characterization. Since we are assuming that R is not alternative, we known that R contains at least two elements a and b such that $d = (a, b) \neq 0$. If $(R, a, b) = 0$, then $d' = (a, ab) = ad \neq 0$. If also $(R, a, ab) = 0$, then, since d, d' are in M, a is in M and $d = 0$ by Lemma 3, a contradiction. Hence a, b may be chosen so that $(a, b) = d \neq 0$ and $(R, a, b) \neq 0$. With a, b so chosen and fixed once for all, define the mapping π (of R into R) by

$$x\pi = (x, a, b), \qquad \text{all } x \text{ in } R. \tag{3.1}$$

Then we may write (2.4) as

$$(wx)\pi = w \cdot x\pi + w\pi \cdot x + (w, x, d). \tag{3.2}$$

THEOREM 1. *Let*

$$N = [n \varepsilon R \mid n\pi = (n, a, b) = 0], \quad S = [s \varepsilon R \mid s\pi = (s, a, b) = sd].$$

Then $R = N + S$, $S \cap N = 0$, $NS = S$, $N \neq 0 \neq S$, and $S^2 = N$.

Proof. (i) Since $d \, \varepsilon \, K \subset N$, $N \neq 0$. Also, S contains $R\pi$ by Lemma 5 so that $S \neq 0$. Now, for any $x \, \varepsilon \, R$, define q by $qd = x\pi$ and observe that $(qd)\pi = q\pi \cdot d$ while $x\pi \cdot \pi = x\pi \cdot d = qd \cdot d$. Hence $q\pi = qd$ and $q \, \varepsilon \, S$. Set $y = x - q$ and obtain $y\pi = x\pi - q\pi = 0$ so $y \, \varepsilon \, N$, and $R = N + S$. Clearly $S \cap N = 0$.

(ii) Note that $(ns)\pi = n \cdot sd + (n, s, d) = ns \cdot d$ so $NS \subset S$. If x is the solution of $nx = s$, $n \neq 0$, then $x = n' + s'$, $n(n' + s') = s$ and $nn' \, \varepsilon \, S$. Thus $nn' \cdot d = (n, n', d)$ so $n' = 0$, $x = s'$ and $NS = S$.

(iii) Finally, $(ss')\pi = sd \cdot s' + s \cdot s'd + (s, s', d) = s \cdot ds' + s \cdot s'd = 0$ by Lemma 4(iv) so that $S^2 \subset N$. The trick which worked in (ii) may be used again to get $S^2 = N$.

LEMMA 6. *With definitions as in Theorem* 1, (i) $ns \cdot d = s \cdot dn$, (ii) $(dn, s) = 0$, (iii)[2] $(N, R, d) = 0$.

Proof. Since $(n, s)\pi = 0$, we have $ns \cdot d = (sn)\pi = sd \cdot n + (s, d, n)$ and this gives (i). Now $dn \cdot s \, \varepsilon \, S$ and $s \cdot dn \, \varepsilon \, S$ by (i) so that $(s, dn) \, \varepsilon \, S$. But $(s, dn) \, \varepsilon \, K \subset N$ so $(s, dn) = 0$. For (iii) we observe that $(n, x, d) = (nx)\pi + n \cdot x\pi$ so (n, x, d) in S. But also $(n, x, d) = (xd, n) + (x, n)d$ and thus $(n, x, d) \, \varepsilon \, K \subset N$. Hence $(n, x, d) = 0$ and this is (iii).

THEOREM 2. *Let N and S be defined as in Theorem* 1. *Then* (i) $N^2 = N$, (ii) $(N, S) = 0$, (iii) $SN = S$, (iv) $N = K$, (v) $(K, R) = 0$ *and K is a field.*

Proof. Lemma 6(iii) implies that $(nn')\pi = 0$ and hence $N^2 \subset N$. The usual maneuver gives $N^2 = N$. Now we observe that any $n' \, \varepsilon \, N$ can be written $n' = dn$ for some n in N. Then, for any s in S, $(n', s) = (dn, s) = 0$ by Lemma 6(ii). Thus $(N, S) = 0$ and $SN = S$.

Using (ii), $0 = (nn', s) = (s, n, n')$ so $(S, N, N) = 0$. Therefore $0 = (sn, n', n'') = s(n, n', n'')$ and thus $(N, N, N) = 0$, $(R, N, N) = 0$. Now, as in the proof of Lemma 3, $(R, n, n') = 0$ implies $(n, n') \, \varepsilon \, M$. But also $(R, n, nn') = 0$ so $(n, nn') \, \varepsilon \, M$. Hence, if $(n, n') \neq 0$, $n \, \varepsilon \, M$, $(n, n') = 0$ by Lemma 3. This contradiction proves $(N, N) = 0$, $(N, R) = 0$. Thus $N \subset K$ by (2.2) and this proves $N = K$. We need only remark that K is a commutative associative division ring to complete the proof.

We collect our results in

---

[2] We are indebted to the referee for the remark, and the proof, that $(N, R, d) = 0$, thus simplifying our original version of this part of the lemma.

THEOREM 3. *Let R be a not alternative right alternative division ring of characteristic two with the properties that*

$$(wx, y, z) = w(x, y, z) + (w, y, z)x + (w, x, (y, z))$$

and $(x, y) \varepsilon K$, the left nucleus of R, for all w, x, y, z of R. Then $R = K + Ks$, K a field, commutative with all of R, and $s \varepsilon R$, $s \notin K$. Moreover, multiplication in R is given by

$$(k_1 + k_2 s)(k_3 + k_4 s) = k_1 k_3 + k_2 \cdot k_4 \theta + (k_1 k_4 + k_2 k_3)s,$$

where θ is an additive endomorphism of K.

Proof. The proof is immediate in view of the foregoing and the observation that $k_4\theta = s \cdot sk_4$ is an additive endomorphism of K.

4. Remarks. It would be interesting to know if all not alternative right alternative division rings have property *ACP* of definition 3. And it would be of interest to determine whether there exist any finite Bruck rings. It is clear, of course, that none can be constructed by the method outlined in the introduction, for no finite field can have characteristic two and also a non-square element.

THE UNIVERSITY OF OREGON.

REFERENCES.

[1] E. Kleinfeld, "Right alternative rings," *Proceedings of the American Mathematical Society*, vol. 4 (1953), pp. 939-944.

[2] R. L. San Soucie, "Right alternative division rings of characteristic two," *ibid.*, to appear.

[3] ———, "Right alternative rings of characteristic two," submitted to *Proceedings of the American Mathematical Society*.

[4] L. A. Skornyakov, "Right alternative fields," *Izvestia Akademiia Nauk SSSR. Seriia Matematichesaia*, vol. 15 (1951), pp. 177-184.

[5] Max Zorn, "Theorie der alternativen Ringe," *Abhandlungen Mathematik Seminar Hamburgischen Universitat*, vol. 8 (1930), pp. 123-147.

g

s,
n-

a-

nt
ld
is
he
n-

cal

id.,

ngs

SR.

mar